3/2020

DVD Deutsche Vereinigung für Datenschutz e.V.

# Datenschutz Nachrichten

43. Jahrgang
ISSN 0137-7767
14,00 Euro



## Elektronische Bezahlsysteme

■ Vom Wald der Bezahl-Systeme und deren Folgen ■ Bitcoins – Anonyme Zahlungsmethode der Zukunft ■ PSD2 – Verbraucherschutz in einer digital vernetzten Gesellschaft ■ Datenschutz in Kenia und wie er sich auf E-Payment auswirkt ■ Eine App, die zu viel kostet ■ Die Tücken der Heimarbeit ■ Nachrichten ■ Rechtsprechung ■ Buchbesprechungen ■

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de

# Inhalt



# Termine



Foto: Pixabay..com

14. bis 16. Oktober 2020
**Online-Konferenz – BvD-Herbstkonferenz & Behördentag 2020 „Daten sammeln: mobil – international – legal(?)“**

Sonntag, 01. November 2020
**Redaktionsschluss DANA 4/2020**
Schwerpunktthema Mobilität

Mittwoch, 04. November 2020
**Online-Tagung „Datenschutz in der Medizin-Update 2020“**

Samstag, 21. November 2020
**Vorstandssitzung** (in Bonn oder virtuell)

Sonntag, 22. November 2020
**DVD-Mitgliederversammlung** (in Bonn oder virtuell)

DANA
**Datenschutz Nachrichten**
ISSN 0137-7767
43. Jahrgang, Heft 3

**Herausgeber**
Deutsche Vereinigung für Datenschutz e.V. (DVD)
DVD-Geschäftsstelle:
Reuterstraße 157, 53113 Bonn
Tel. 0228-222498
IBAN: DE94 3705 0198 0019 0021 87
Sparkasse KölnBonn
E-Mail: dvd@datenschutzverein.de
www.datenschutzverein.de

**Redaktion (ViSdP)**
Dr. Susanne Holzgraefe, Frank Spaeing
c/o Deutsche Vereinigung für Datenschutz e.V. (DVD)
Reuterstraße 157, 53113 Bonn
dvd@datenschutzverein.de
Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autorinnen und Autoren.

**Layout und Satz**
Frans Jozef Valenta, 53119 Bonn
valenta@datenschutzverein.de

**Druck**
Onlineprinters GmbH
Rudolf-Diesel-Straße 10
91413 Neustadt a. d. Aisch
www.diedruckerei.de
Tel. +49 (0) 91 61 / 6 20 98 00
Fax +49 (0) 91 61 / 66 29 20

**Bezugspreis**
Einzelheft 14 Euro. Jahresabonnement 48 Euro (incl. Porto) für vier Hefte im Kalenderjahr. Für DVD-Mitglieder ist der Bezug kostenlos. Das Jahresabonnement kann zum 31. Dezember eines Jahres mit einer Kündigungsfrist von sechs Wochen gekündigt werden. Die Kündigung ist schriftlich an die DVD-Geschäftsstelle in Bonn zu richten.



**Leserbriefe**
Leserbriefe sind erwünscht. Deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

**Abbildungen, Fotos**
Frans Jozef Valenta,
Pixabay, iStock

# Editorial

Im Geschichtsunterricht wird gelehrt, dass alles mit dem Tauschhandel angefangen hat. Die Älteren unter uns erinnern sich vielleicht noch, dass besonders nach dem Krieg der Tauschhandel wiederauflebte. Ist diese Zeit wirklich vorbei? Wenn beide Seiten vom jeweils anderen profitieren können, ist der Tauschhandel noch üblich.

Die Geschichte lehrt uns aber auch, dass die Sache mit dem direkten Tauschhandel seine Grenzen hat. Münzen wurden eingeführt, die als Tauschmittel genutzt wurden. Das Bargeld entstand. Im Laufe der letzten Jahrzehnte wurden die Möglichkeiten elektronischer Bezahlung immer weiter ausgebaut. Aber Vorsicht, ist das Bezahlen mit Bargeld noch anonym möglich, so sieht das bei der elektronischen Bezahlung (E-Payment) schon anders aus. Was für die DVD der Anlass ist, E-Payment als Schwerpunktthema des vorliegenden Heftes zu wählen.

Der Artikel „Vom Wald der Bezahlsysteme und deren Folgen“ durchleuchtet gängige elektronische Bezahlsysteme, „Bitcoins – Anonyme Zahlungsmethode der Zukunft“ befasst sich damit, wie die neuen BaFin-Regelungen Bitcoins betreffen, in der Studie zu M-PESA wird vorgestellt, wie in Kenia mit dem Smartphone bezahlt wird. Natürlich darf beim Thema E-Payment ein Artikel zu PSD2 nicht fehlen. Wer viel in London, Brüssel oder den Niederlanden unterwegs ist, kennt vielleicht bereits die hier unter die Datenschutzlupe genommene Oystercard, OV-Chipkaart oder MoBIB-Karte, elektronische Bezahlsysteme für Fahrten mit öffentlichem Nahverkehr. Ein Bericht über die Datenschutzentwicklung in Kenia und wie sich das auf dortige elektronische Bezahlmöglichkeiten auswirkt, schließen das Thema E-Payment ab.

Es folgen aus weiterhin aktuellem Anlass Artikel zum Thema Corona und zu gesellschaftlichen Themen. Die Kontaktnachverfolgung in Coronazeiten sowie die Corona-Warn-App an sich und die App-Nutzung im Beschäftigungsverhältnis werden in Artikeln genauer untersucht. Der Bericht „PimEyes & Gesichtserkennung in Europa“ sowie ein Bericht zu Fingerabdrücken im Personalausweis runden das Heft ab.

Nachrichten rund um Datenschutz, aktuelle Rechtsprechungen sowie Buchbesprechungen befinden sich wie gewohnt am Ende des Heftes. Wir wünschen viel Freude beim Lesen.

## Autorinnen und Autoren dieser Ausgabe:

**Heinz Alenfelder**
Vorstandsmitglied in der DVD, alenfelder@datenschutzverein.de, Köln

**Leopold Beer**
Jura-Student und freier Journalist, LeopoldBeer@gmx.de

**Raik Borkowski**
Experte für Open Banking und PSD2, TME AG, borkowski@tme.ag

**Friedemann Ebelt**
Campaigner DigitalCourage e. V., friedemann.ebelt@digitalcourage.de

**Maike Grahneis**,
Wirtschaftsjuristin LL.M., Datenschutzberaterin bei der ds² Unternehmensberatung GmbH & Co. KG, Maike.Grahneis@ds-quadrat.de

**Dr. Susanne Holzgraefe**
Vorstandsmitglied in der DVD, holzgraefe@datenschutzverein.de

**Victor Masyula**
Diplom-Informatiker aus Kenia, victormasyula@gmail.com

**Stephan A. Paxmann**
Gründer und Vorstand der TME AG, paxmann@tme.ag

**Julia Reda**
Gesellschaft für Freiheitsrechte e.V., julia.reda@freiheitsrechte.org

Dr. Susanne Holzgraefe

# Vom Wald der Bezahl-Systeme und deren Folgen

Münzen werden schon seit vielen Jahrhunderten als Tausch gegen Ware und Dienstleistungen eingesetzt. Später kamen dann die Scheine dazu. In der modernen Welt wird das Bargeld immer mehr verdrängt und durch elektronische Bezahlmöglichkeiten ersetzt. Es ist ja auch irgendwie praktisch, einfach die Armbanduhr vor ein Gerät zu halten, um die eingekaufte Ware zu bezahlen. Kein lästiges Herumschleppen schwerer Münzsäcke, dicker Portemonnaies oder klobiger Handys mehr.

Münzen und Scheine sind schon immer durch viele Hände geflossen und galten als Bakterienschleudern. Die Corona-Zeiten haben viele Menschen für die Unreinheit des Bargeld-Materials sensibilisiert. Geschäfte, die sonst nur zähneknirschend etwas anderes als Bargeld annahmen, bitten plötzlich, möglichst kontaktlos zu bezahlen. Es gibt sogar Geschäfte, die bar bezahlen wollende Kunden an die Konkurrenz verweisen, weil sie selbst Angst vor Bakterien und Viren auf dem Bargeld haben. Es wird also höchste Zeit, sich mit den Folgen elektronischer Bezahlung auseinander zu setzen.

Der Wald der Bezahlmöglichkeiten ist riesig. Genauer unter die Datenschutz-Lupe genommen werden in diesem Artikel, neben einleitenden Worten zum Bargeld und der guten alten Vorkasse, die Bezahlung per Überweisung, Giro- und Kreditkarte, Bitcoin, Apple Pay, PayPal und Klarna sowie Paysafe und MyCard2Go.

Darüber hinaus wird am Ende noch kurz auf das Thema Löhne und Gehälter und die Weitergabe von Informationen an staatliche Stellen eingegangen.

Anzumerken ist hier noch, dass bei der Recherche nur Apple Pay, nicht Google Pay unter die Lupe genommen wurde. Die Recherchen von Bank- und Kreditkarte beschränken sich auf die Commerzbank, Visa- und Mastercard.

## Bargeld und Barzahlung

Der Vorteil von Bargeld ist die Anonymität. Solange mich die Händlerin nicht persönlich kennt oder mir die Sachen liefert, ich die gekaufte Ware weder jemandem zeige noch davon erzähle, weiß niemand, was ich mit meinem Bargeld gekauft habe oder wie teuer es war. Es geht ja auch niemanden etwas an. Die Händlerin kennt mich vielleicht und hat in ihrem Gedächtnis abgespeichert, dass ich Kondome gekauft habe. Ohne weiter darüber nachzudenken, erkundigt sie sich bei meinem Mann nach der Qualität der Kondome, doch dieser weiß gar nichts von den Kondomen. Tja, damit hätte ich rechnen und es verhindern können, indem ich die Kondome dort gekauft hätte, wo mich niemand persönlich kennt. Dennoch bleibe ich bei der Bezahlung mit Bargeld weitestgehend unerkannt.

Selbst bei Bestellungen im Internet ist Barzahlen möglich. Wie das funktioniert? Die Ware wird online bestellt und bei den Bezahlmöglichkeiten Barzahlen ausgewählt. Bei Abschluss der Bestellung gibt es einen Barcode. Mit diesem Barcode lässt sich die Ware in einem der teilnehmenden Geschäfte vor Ort bar bezahlen. Sobald die Ware bezahlt ist, wird der Auslieferungsprozess gestartet. Weitere Informationen dazu gibt es auf barzahlen.de. Das einzige, was die Händlerin weiß, ist, dass sie eine Lieferung an eine Adresse geschickt hat. Ob das jetzt die Adresse der Person war, die die Ware bezahlt hat, oder eine andere Adresse, kann die Händlerin nicht verifizieren.

In Corona-Zeiten ist es bei der Barzahlung bei Onlinebestellungen zu empfehlen, sich vorher zu erkundigen, ob das Geschäft in der Nähe, in dem die Ware später bar bezahlt werden soll, zu denen gehört, die die Annahme von Bargeld verweigern, um nicht am Ende doch mit einer Karte bezahlen zu müssen.

## Vorkasse

Daneben gibt es auch noch das Bezahlen per Vorkasse beim Paket- bzw. Lieferdienst. Egal, ob die Kleidung aus dem Katalog, die Türbeschläge aus dem Internet oder die Pizza – der Bote händigt die Ware erst aus, wenn sie an der Tür bezahlt wird. Solange die Bezahlung bar passiert, werden nur die Boten zu Mitwissenden. Allerdings kennen die mit der Lieferung Beauftragten lediglich die Summe und die äußeren Paketabmessungen. Der Inhalt ist ihnen weitestgehend unbekannt. Selbst wenn sichtbar auf dem Pizzakarton „glutenfrei“ steht, heißt das nicht, dass die Pizza auch für die Person bestimmt ist, die die Pizza an der Tür entgegengenommen hat. Vor allem heißt das nicht, dass die Pizza zwingend für eine unter Zöliakie leidende Person ist. Genauso wenig, wie die Essensbox für Kinder, die bei einem Essenlieferanten bestellt wird, zwangsweise wirklich für ein Kind ist. Es ist für Erwachsene nicht schädlich, ein für Kinder vorgesehenes Essen zu verspeisen.

Solange die Vorkasse bar abgewickelt wird, ist auch hier der Kreis der Mitwissenden überschaubar. Rückschlüsse auf irgendwelche Vorlieben, gesundheitliche Einschränkungen, Schuhgrößen oder ähnliches kann die Händlerin zwar zur Lieferadresse ziehen, aber die bei der Lieferadresse angegebene Person ist nicht zwangsweise die Person, für die die Ware bestimmt ist. Der Bote kann noch weniger Rückschlüsse ziehen, da er ja in der Regel den genauen Inhalt von Paketen nicht kennt.

Dennoch gibt es hier neben der Händlerin noch die mit der Lieferung Beauftragten, die die Anonymität schwächen. Wird immer derselbe Bote geschickt bzw. dasselbe Unternehmen mit der Lieferung beauftragt, so wissen die Lieferanten durchaus, wohin derselbe Händler häufiger liefert. Je nach Ware wissen sie zum Beispiel, dass sie an Person X wöchentlich einen Blumenstrauß liefern oder Person Y alle zwei Tage eine Pizza erhält und Person Z zweimal pro Woche ein großes Paket vom selben Versandhändler.

Hier zeigt sich schon, wie wichtig der in der DSGVO geforderte Auftragsver-

arbeitungsvertrag zwischen Händlerin und extern beauftragten Lieferanten ist. Aber selbst wenn sich das juristisch lösen läßt, bleibt der entstandene Schaden durch zu viel Tratsch und sowohl falsche Rückschlüsse als auch möglicherweise durchaus richtige Folgerungen, die sich nicht rückgängig machen lassen. Informationen, die einmal bekannt wurden, lassen sich nur schwer entfernen und schon gar nicht aus den Köpfen der Menschen löschen.

Wird die Vorkasse elektronisch abgewickelt, kann es, wie im weiteren Verlauf des Artikels erläutert wird, weit mehr Mitwissende geben, die die Anonymität weiter schwächen.

**Überweisung und Girokarte**

Bis in die 90er waren neben der Überweisung auch noch Wechsel und Papier-Schecks gängige Zahlungsmittel. Schon damals wurden die Banken dadurch Mitwissende, wer mit wem Geschäfte tätigte. Das Bankgeheimnis sollte hier schützen. Darüber hinaus erfuhren beide Parteien, bei welcher Bank der Andere ist. Das ist eine zusätzliche, persönliche Information, die den jeweils Anderen eigentlich nichts angeht und die nicht zwingend zum Geschäftsabschluss erforderlich ist.

Der Papier-Scheck wurde 2002 ganz durch die Debit-Karte ersetzt. Hierfür kamen dann auch Kartenlesegeräte auf den Markt. Die Geräte werden nicht von den Banken hergestellt, sondern es gibt sehr viele verschiedene Anbieterinnen, die Kartenlesemöglichkeiten und ggf. entsprechende Geräte für ihre Lösungen anbieten. Zumindest bei einigen Anbieterinnen bekommen die Händler monatliche Abrechnungen, aus denen hervorgeht, von welchen Konten und in welcher Höhe Gelder geflossen sind.

Das bedeutet, dass jetzt nicht mehr nur die Banken die Informationen nachvollziehen können, wer von wem Geld bekommen und wer an wen Geld überwiesen hat, sondern auch die entsprechenden Kartenlese-Anbieterinnen.

Darüber hinaus werden die Daten auch noch irgendwie zwischen dem Lesegerät und der Bank übertragen; per Internet, per Fax, per Telegramm … der Fantasie sind hier kaum Grenzen gesetzt.

Für Kartenlesegeräte und deren Übertragung gibt es Standards. Aber, ein Standard ist kein Gesetz. Ein Standard ist freiwillig. Standard bedeutet, es haben sich zum Beispiel eine Herstellerin, ein Wissenschaftlerin und eine Produktanwenderin zusammengesetzt und überlegt, einen Standard zu entwickeln. Ob alle Anderen dem Standard jetzt folgen oder ihre eigenen Ideen umsetzen, bleibt den Herstellenden überlassen.

Ist die Übertragung vom Kartenlesegerät über ggf. die Anbieterin zur Bank komplett und immer verschlüsselt? Und wenn ja, was für Verschlüsselungsmethoden wurden verwendet? Bei der Recherche für diesen Artikel konnten die Händlerinnen, bei denen vor Ort nachgefragt wurde, zum Thema Verschlüsselung bei der Übertragung von ihrem Kartenlesegerät gar nichts sagen. Die Herstellerinnen, bei denen telefonisch nachgefragt wurde, versicherten alle, dass selbstverständlich die Übertragung komplett verschlüsselt sei, aber auf die Frage nach der Methode verwiesen sie auf das Geschäftsgeheimnis.

Positiv denkend sind bei der Bezahlung mit Girokarte lediglich zusätzlich die Banken und die Lesegerät-Anbietenden die Mitwissenden. Beide können nachvollziehen, wer mit wem Geschäfte in welcher Höhe macht.

Überweisungen auf Papier werden heutzutage in der Bankfiliale elektronisch erfasst. Daneben lassen sich Beträge per Online-Banking und am Geldautomaten überweisen. So oder so sind die Banken hier Mitwissende. Stellen die Banken die verwendete Software selbst her? Kaufen sie sie zu? Gibt es da noch eine Zwischenspeicherung zu den Transaktionen bei Software-Herstellern? Und wie sieht das hier mit der Transport-Verschlüsselung aus? Hat hier eventuell eine Auftragsverarbeiterin zusätzlich Einblick?

Die Datenschutzerklärung vom Online-Banking-Portal der Commerzbank sagt: *„Innerhalb der Bank erhalten diejenigen Stellen Zugriff auf Ihre Daten, die diese zur Erfüllung unserer vertraglichen und gesetzlichen Pflichten brauchen. Auch von uns eingesetzte Dienstleister und Erfüllungsgehilfen können zu diesen Zwecken Daten erhalten, wenn diese insbesondere das Bankgeheimnis wahren. Dies sind Unternehmen in den Kategorien kreditwirtschaftliche Leistungen, IT-Dienstleistungen, Logistik, Druckdienstleistungen, Telekommunikation, Inkasso, Beratung sowie Vertrieb und Marketing."*

Weiter unten steht zu den Empfängern der Daten unter anderem noch: *„Dienstleister, die wir im Rahmen von Auftragsverarbeitungsverhältnissen heranziehen."*

Das sind schon ganz schön viele potentielle Stellen, die ggf. Einblick bekommen, wer mit wem Geschäfte macht. Stellen, die anhand des Verwendungszweckes spekulieren könnten, worum es bei den Geschäften geht. Bei dem Verwendungszweck ‚Gehalt' könnte vermutet werden, dass die Geldgeberin die Arbeitgeberin ist. Bei einem Geldtransfer, dessen Verwendungszweck auf Bezahlung von gekauften Produkten aus einem Sexspielzeugversand hinweist, ist die Wahrscheinlichkeit sehr groß, dass es sich bei dem Kauf, um eines oder mehrere im öffentlich einsehbaren Versandkatalog angebotene Produkte handelt. Natürlich lassen sich auch Rückschlüsse unterschiedlichster Art bei dem Verwendungszweck ‚Unterhalt für Max' ziehen.

Aus einem häufigen Geldtransfer zu Fastfoodketten könnte auf ungesunde Ernährung geschlossen werden, zu einer Apotheke auf gesundheitliche Probleme und zu einer Fahrschule je nach Höhe der Beträge und Wiederholung der Zahlungen darauf, dass die Sache mit dem Führerschein leichter oder schwerer fiel.

Banken unterliegen strengen staatlichen Kontrollen. Von einer durchgehenden Verschlüsselung sowie der technischen Unterbindung unabsichtlicher Übertragungen an große, US-amerikanische IT-Konzerne sollten Kunden ausgehen dürfen. Darüber hinaus weist zumindest die Commerzbank ja schon in dem oben zitierten Ausschnitt aus ihrer Datenschutzerklärung im Online-Banking-Portal darauf hin, dass sie alle Beteiligten zur Wahrung des Bankgeheimnisses verpflichtet hat.

**Bankeinzug / Lastschrift**

Der Betroffene erteilt dem Empfänger die Erlaubnis den ausstehenden Betrag per Bankeinzug einzuziehen. Hier wird

häufig der Einzug von mehreren Betroffenen gebündelt und allein mit dem Kontoauszug lässt sich die Identität der Betroffenen nicht feststellen. Erst wenn der Einzug nicht klappt oder Betroffene dem Einzug widersprechen bzw. ihn zurückziehen, sind Angaben zum Betroffenen ersichtlich. Dennoch weiß natürlich der Empfänger, wer alles an seinem Bankeinzug teilnimmt.

Auch die Banken und ggf. ihr Gefolge wissen natürlich genau, von wem sie das Geld zu welchem Verwendungszweck einziehen.

Setzt die Empfängerin noch externe Dienstleistende, wie Steuerberatungs-Kanzleien, ein, die sich um die Verwaltung der Einzüge kümmern, so ist das eine weitere Mitwisser-Quelle.

**Kreditkarten**

Bei der Zahlung mit Kreditkarte erweitert sich der vorgenannte Kreis der Mitwissenden noch um die jeweiligen Kreditkarten-Institute und deren gesamte Auftragsverarbeitende.

Auch wenn hier natürlich Alle strengsten Auflagen unterliegen und verschiedene Gesetze und Vorschriften zum Stillschweigen verpflichten, wird der Personenkreis, der Umgang mit den Informationen hat, nicht nur immer größer, sondern auch immer unübersichtlicher.

Wie viele einzelne Personen sind es, die einsehen können, dass ich einmal im Monat im Schuhgeschäften bestimmte Summen an Geld ausgebe? Sind es zehn Personen, sind es hundert Personen oder ist die Liste schon mehrere Seiten lang?

Selbst wenn sie alle vertraglich und gesetzlich verpflichtet wurden, wächst mit jeder weiteren Person, die Kenntnis über die Informationen hat, die Wahrscheinlichkeit eines Maulwurfs.

Nichtsdestotrotz ist die Bezahlung mit Kreditkarte natürlich eine bequeme Sache. Mit vielen Kreditkarten lässt sich im Gegensatz zur Girokarte auch außerhalb Europas problemlos bezahlen und sie werden weltweit von vielen Bargeldautomaten akzeptiert.

Egal, ob mal eben schnell den Flug buchen oder umbuchen, Tickets für das Musical am selben Abend in London reservieren oder Bargeld in Nagasaki am Geldautomaten ziehen, um weiter durch das Bargeldland Japan zu reisen, Kreditkarten sind einfach in vielen Situationen praktisch.

Die Tatsache, dass die Kreditkarten in Deutschland üblicherweise nur einmal im Monat das Konto belasten, kann auch von Vorteil sein. So kann zum Beispiel die BahnCard schon bestellt und genutzt werden, bevor das Gehalt auf dem Konto ist und tatsächlich wird der Betrag erst nach Gehaltseingang abgebucht.

Eine Kreditkarte ist praktisch. Sich dessen bewusst zu sein, dass neben den Geldempfängern auch Banken und Kreditinstitute samt Gefolge Zahlungen und Gewohnheiten nachvollziehen können, ist wichtig.

Welche Folgen kann es haben, dass so viele wissen, dass ich jeden Monat eine gewisse Summe in Schuhgeschäften ausgebe? Angefangen damit mit Schuhwerbung auf allen Wegen zugebombt zu werden, könnte ein Fetisch für Schuhe unterstellt werden und dieser Ruf weitere Unannehmlichkeiten nach sich ziehen. Ergeben weitere Recherchen, dass überwiegend hohe Absatzschuhe in derselben Größe gekauft wurden, könnten die häufigeren Einnahmen von Taschengeld durch erotisch-sexuelle Dienste unterstellt werden usw.

**Apple Pay**

Apple Pay beginnt damit, dass Kreditkarten im sogenannten Wallet hinterlegt werden. Wobei hier nicht wirklich die Kreditkarten hinterlegt werden, sondern, wie nachfolgend beschrieben, ein verschlüsselter Gerätecode. Wallet ist eine Verwaltungssoftware für Kreditkarten und alle möglichen Arten von Tickets. Zum Beispiel Boarding-Pässe für Flüge, Eintrittskarten für Schwimmbäder, Tickets für Musicals und so weiter. Das englische Wort *'wallet'* bedeutet *'Brieftasche'*.

Für Kreditkarten und neuerdings auch Girokarten wird mit Hilfe der Software 'wallet' ein von der Bank verschlüsselter Datensatz, der einen eindeutigen Gerätecode enthält, in der Nutzer-Cloud abgelegt. Also an einem Ort abgelegt, auf den die Wallet-Software von allen Geräten des Nutzers zugreifen kann. So ist es möglich, dass die Karten und Tickets sowohl mit dem Laptop, dem Tablet, dem Smartphone als auch der Uhr abrufbar sind und genutzt werden können.

Wie bei Apple üblich, gibt es auch zu Apple Pay eine sehr ausführliche und gut verständliche Beschreibung zum Thema Datenschutz und Sicherheit[1], die sich am einfachsten durch die Suchbegriffe *'Apple Pay Datenschutz'* finden lässt.

In der Erklärung wird noch einmal explizit darauf hingewiesen, dass Apple keine einzelne Informationen wie Kartennummer oder Inhaber speichert und auch die Geräte keine derartigen Informationen übertragen. Wie das im einzelnen funktioniert, lässt sich an oben genannter Stelle nachlesen. Kurz gesagt ist alles verschlüsselt und nur die Bank, zu der das Konto hinter der Kreditkarte gehört, hat den Schlüssel.

Damit nicht aus Versehen mit der Uhr oder dem Smartphone im Vorbeigehen bezahlt wird und um Missbrauch zu vermeiden, kann die Karte nur nach Gesichtserkennung, Fingerabdruckscan oder Eingabe eines Codes aufgerufen werden. Darüber hinaus ist bei der Uhr und bei der Gesichtserkennung vor dem Bezahlen noch ein Seitenknopf zweimal zu drücken.

Es ist natürlich sehr praktisch, den Supermarkt-Einkauf einfach per Uhr zu bezahlen. Weder müssen die Karten selbst noch das große Smartphone mitgenommen werden. Bei Online-Bestellungen auf Apple Pay zu klicken erspart die Eingabe der Kreditkarten-Daten.

Auch bei Online-Käufen legt Apple höchsten Wert auf Sicherheit und Datenschutz.

Apple kann nach Abschluss der Transaktion nicht nachvollziehen, wer bei wem was gekauft hat. Sie speichern zu statistischen Zwecken Auswertungen und zur Verbesserung von Apple Pay die Beträge und die Geldempfänger, aber keinerlei Informationen zu den Bezahlenden.

Jedoch erhalten das Kreditinstitut und die Banken dieselben Informationen, die sie auch per Bezahlung mit Kreditkarte bekommen würden. Darüber hinaus kann die Bank nachvollziehen, dass mit Apple Pay bezahlt wurde. Auf den Kontoauszügen der Kreditkarte gibt es zumindest bei der Commerzbank keinen Hinweis, wann via Apple Pay und wann anders bezahlt wurde.

Apple Pay ist einfach nur ein Durchläufer, der dafür sorgt, dass die Origi-

nalkarten und ggf. auch das Handy zu Hause bleiben dürfen.

### PayPal und Klarna

PayPal wird EU-weit als Bank geführt und die luxemburgische Bankaufsicht, Commission de Surveillance du Secteur Financier (CSSF), ist die zuständige Aufsichtsbehörde.

Klarna ist das schwedische Gegenstück zu PayPal mit Vollbanklizenz unter schwedischer Aufsicht. Für Festgeldanlagen, die zusätzlich möglich sind, hat Klarna sich daneben gemäß EU-Recht bei der deutschen Bankenaufsicht registrieren lassen.

Um Paypal oder Klarna nutzen zu können, muss ein Konto oder eine Kreditkarte hinterlegt werden. Es können auch mehrere Konten bzw. Karten in einem Benutzerkonto hinterlegt werden.

Paypal bezahlt die Rechnung und zieht das Geld per Bankeinzug oder über die Kreditkarte ein. Darüber hinaus kann Guthaben an PayPal bezahlt werden und kommende Rechnungen können dann mit dem Guthaben beglichen werden. Stornierungen enden als PayPal-Guthaben. Das Guthaben kann aber auch einfach auf das hinterlegte Konto oder die Kreditkarte transferiert werden.

Dem Kunden wird eine Übersicht bereit gestellt, an wen genau wie viel Geld gezahlt wurde: ein Paypal-Kontoauszug. Wurde nicht per Paypal-Guthaben bezahlt, sondern hat Paypal sich das Geld direkt von der Kreditkarte oder dem Konto genommen, so ist auf dem entsprechenden Kontoauszug des Bankkontos bzw. der Kreditkarte zu erkennen, an wen das Geld ging. Paypal reicht die Empfängerdaten an die Bank durch.

Somit sind Paypal bzw. Klarna weitere Mitwisser im Bezahlprozess. Die Bank und ggf. das Kreditkarteninstitut wird nur dann nicht mehr zum Mitwisser, wenn Paypal per Guthaben bezahlt. Dadurch bekommen Bank und Kreditkarteninstitut nur mit, dass Geld an Paypal gezahlt wurde, nicht aber, an wen via Paypal Geld geschickt wurde.

Der große Vorteil von Paypal und Klarna liegt darin, dass keine Informationen zum Bankkonto oder der Kreditkarte an Zahlungsempfänger weitergegeben werden.

### Paysafecard

Paysafecard ist ein irisches Unternehmen mit Banklizenz. In Filialen von verschiedenen großen Supermarktketten und Tankstellen lässt sich die Paysafecard mit einem Guthaben zwischen zehn und hundert Euro erwerben. Auf paysafecard.com lassen sich durch Eingabe von Postleitzahl und Ort die Verkaufsstellen in der Umgebung finden. Der Zettel sieht auf den ersten Blick aus wie ein Kassenbon. Mit dem dort abgedruckten Code lässt sich nun im Internet bezahlen, bis das Guthaben aufgebraucht ist.

Das klingt erstmal nach einer bargeldlosen, anonymen Lösung. Doch so anonym ist Paysafecard dann doch nicht. Paysafecard versucht an die IP-Adresse seiner Kunden zu kommen. Der Grund dafür ist einfach: Das Unternehmen besitzt eine Banklizenz. Das Schwesterunternehmen, die britische Prepaid Services Company Limited, wird von der Behörde Financial Conduct Authority (FCA) reguliert. Das bedeutet, sie sind dazu verpflichtet, gegen Geldwäsche und andere juristische Verstöße aktiv vorzugehen.

Der Journalist Lars „Ghandy" Sobiraj hat 2017 in seinem Blog, tarnkappe.info[2], über seine Versuche berichtet, die Paysafecard erfolglos mit Tor-Browser und auch diversen, die IP verschleiernden, VPN-Anbietern zu nutzen.

Fazit: Paysafecard versucht an die IP seiner Kunden zu kommen. Gelingt das nicht, sperrt Paysafecard die Karte. Die Freischaltung ist dann nur durch ein Identifizierungsverfahren möglich. Auf diese Weise wird bei einer Geschäftsabwicklung das Unternehmen Paysafecard samt Gefolge zum Mitwisser.

### mycard2go

Der anonyme mycard2go-Serivce wurde am 31. Mai 2020 komplett eingestellt. Hierbei handelte es sich um eine aufladbare Prepaid Kreditkarte. Auch hier war das Limit pro Aufladung 100 Euro. Das ist eine gesetzlich vorgeschriebene Maximalhöhe aus dem Geldwäschegesetz. Aufgeladen werden konnte die Karte unter anderem in bar an verschiedenen Tankstellen, in Kiosken und Geschäften.

Ab 2017 bedurfte es dann auf Grund gesetzlicher Vorschriften einer Identifizierung für die Karte.

Bei der Recherche für diesen Artikel im Januar 2020 teilte eine Mitarbeiterin telefonisch mit, dass die anonymen Karten nicht mehr erworben, sondern nur noch vorhandene Karten aufgeladen werden könnten. Die Gesetzgebung lasse hier keinen Spielraum.

### Anonyme Kreditkarte

Es gibt durchaus aufladbare Kreditkarten, für die es keiner Identifizierung bedarf. Allerdings nicht in Deutschland. Aufladbare Kreditkarten gibt es u.a. von Visa. Allerdings wird der Kunde hier in Deutschland zu einer Identifizierung gezwungen. Wodurch sowohl die Bank als auch das Kreditkarteninstitut samt dem jeweiligen Gefolge zu Mitwissern werden und der Unterschied zur nicht-anonymen-Kreditkarte lediglich darin besteht, dass die Kreditkarte Prepaid ist und Händlerinnen anhand der Kartendaten den Kartenbesitzer nicht identifizieren können.

### Geldchip-Karten

In einigen chinesischen Regionen ist es üblich, dass Löhne und Gehälter nicht in Scheinen und Münzen ausgezahlt werden, sondern der Betrag auf eine Chipkarte gespielt wird, die dann wiederum in Geschäften usw. zum Bezahlen genutzt werden kann.

In Deutschland wurden seit Ende der 90er Jahre Geldchips auf EC-Karten bzw. Geldchip-Karten in Umlauf gebracht. Das System hat sich allerdings nicht durchgesetzt. War es seiner Zeit vielleicht einfach nur voraus?

Wäre das eventuell die Möglichkeit, eine bargeldlose Bezahlmöglichkeit zu haben, die bezüglich der Anonymität dem Bargeld gleich kommt? Oder ist bei bargeldloser Bezahlung immer zwangsweise eine Identifizierung von Sendern und Empfänger durch Regulierungsbehörden notwendig?

### Mobile Geldverwaltung-Apps

Wie der Artikel zu M-PESA in Kenia zeigt, sind darüber hinaus auch noch mobile Geldverwaltung-Apps im Umlauf. Selbst in Kenia ist die Nutzung ohne Registrierung nur bedingt möglich. Die App hat es auch nach Rumäni-

en und Albanien geschafft[3]. Doch in der übrigen EU verhindern strenge Regulierungen die Einführung. Anonym bezahlen per Handy oder zukünftig per Uhr ist in der EU derzeit nicht vorgesehen.

Bei dem M-PESA-Modell aus Kenia sind bei Registrierung neben den Banken auch noch Mobilfunkanbieter Mitwissende (siehe zu M-PESA auch den Artikel ab Seite 147).

## Bitcoin

Zum Abschluss gibt es noch die Möglichkeit der Bezahlung mit Kryptowährung. Doch wie sieht das hier mit der Anonymität aus? Während der Recherchen kamen neue Vorschriften von der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) heraus, die Kryptowährungen wie Bitcoin treffen.

Leopold Beer hat dem Thema einen eigenen Artikel (ab Seite 145) gewidmet.

## Staatliche Stellen

Neben Banken und Kreditinstituten verschafft sich der Staat immer mehr Einblick in die Finanzen der Menschen. Also noch mehr Mitwissende, dass ich monatlich eine bestimmte Summe in Schuhgeschäften lasse, mehrfach wöchentlich Lebensmittel geliefert bekomme, regelmäßig ins Schwimmbad gehe, viele Bahntickets kaufe und so weiter, und so weiter.

Wie lange kann sich der Widerstand gegen eine Abschaffung des Bargeldes noch halten? Einige europäische Länder haben bereits Centstücke abgeschafft. Nicht mehr mit Bargeld bezahlen zu können ist in einigen Nachbarländern durchaus nichts Neues.

Natürlich ist die Bezahlung mit Uhr cooler und auch bequemer. Aber zu welchem Preis?

Wie sieht die gleichwertig liberal-anonyme Alternative zum Bargeld aus, die das Bargeld ersetzen könnte?

Gibt es durch die strengen Auflagen und Überwachungen bei jeglicher bargeldloser Form der Bezahlung eventuell in Zukunft einen Rückschritt zum Bargeld?

## Löhne und Gehälter

In vielen deutschen Arbeitsverträgen steht, dass die Zahlung des Gehaltes bargeldlos erfolgt. In die Praxis umgesetzt geschieht das üblicher Weise per Überweisung. Neben den Banken und ihrem Gefolge, die hierbei zu Mitwissenden werden, ist es nicht selten, dass die Verwaltung und Überweisung von Gehältern durch externe Stellen wie Steuerberatungs-Kanzleien durchgeführt wird.

Das bedeutet, dass nicht nur Banken und deren Gefolge Mitwissende von personenbezogenen Gehaltsinformationen sind, sondern auch externe Dienstleister der Arbeitgeberin; und zwar nicht nur, wie bei den Banken, was die Höhe der Auszahlung betrifft, sondern darüber hinaus noch wer wo krankenversichert ist, bei wem wieviele Steuern und Sozialversicherungen abgezogen werden, wieviel Bonus es gab, wie hoch die gezahlte Kirchensteuer ist und vieles mehr.

Wird das Gehalt bar ausgezahlt oder auf einen anonymen Geldchip übertragen, ist zumindest erstmal die Bank mit gesamtem Gefolge als Mitwissende ausgeschaltet. Für staatliche Stellen ist es natürlich einfacher Geldeingänge auf einem Konto zu beobachten als Abrechnungen einzufordern.

Dennoch, die Barzahlung von Gehältern ist auch in Deutschland noch erlaubt. Ob sich zukünftig in Deutschland die Auszahlung von Löhnen und Gehältern auf anonyme Geldchips durchsetzt, bleibt abzuwarten. Gesetze, die für Gehaltszahlungen auf anonyme Geldchips keine bzw. reelle Limitierung der aufgeladenen Summe vorsehen, könnten hier helfen.

Spannend ist übrigens auch die Frage, ob ein Unternehmen Bewerber ablehnen darf, nur weil sie den Passus mit der bargeldlosen Bezahlung im Arbeitsvertrag gestrichen haben und ihr Gehalt in bar bekommen möchten.

## Fazit

Der Wald der Bezahlsysteme ist umfangreich. Allerdings sorgen Gesetze und Vorschriften dafür, dass kein einziges Bezahlsystem ähnlich anonym nutzbar ist wie das Bargeld. Nicht nur für Banken und Kreditinstitute werden die Kunden immer gläserner, sondern auch der Staat erhält immer mehr Einblick in unseren Umgang mit finanziellen Mitteln.

Ob das Bargeld in Zukunft abgeschafft oder es auf Grund der zu großen Mitwisserschaft und Überwachung einen Rückschritt zum Bargeld gibt, weil Gesetze und Vorschriften nicht für eine akzeptable gleichwertig-anonyme elektronische Bezahlmöglichkeit sorgen, wird die Zukunft zeigen.

1 https://support.apple.com/de-de/HT203027

2 https://tarnkappe.info/paysafecard-anonymitaet-war-gestern/

3 https://www.welt.de/wirtschaft/bilanz/article162694583/Afrika-zeigt-der-Welt-wie-mobiles-Bezahlen-geht.html

Leopold Beer

# Bitcoins – Anonyme Zahlungsmethode der Zukunft?

## Eine Analyse der Anonymität bei Kryptowährungen sowie der regulatorischen Anforderungen durch BaFin und KWG

Kryptoassets und vor allem Bitcoins sind derzeit in aller Munde. Von den einen als Zahlungsmethode der Zukunft in den Himmel gepriesen, von den anderen als Instrument zur anonymen Begehung von Straftaten abgestempelt, bieten Kryptowährungen eine große Bandbreite an Diskussionsstoff. Eine Frage, die jedoch immer wieder auftaucht und von herausragender Bedeutung sein dürfte, ist, wie sicher das Traden mit Bitcoins ist und wie es um die weitgerühmte Anonymität bei Transaktionen von Bitcoins steht. Zudem sind im Zusammenhang mit Kryptowährungen inzwischen zahlreiche regulatorische Anforderungen zu berücksichtigen, die zuletzt in einer Neufassung des Kreditwesengesetzes („KWG") Gestalt angenommen haben und durch die Bundesanstalt für Finanzaufsicht („BaFin") überwacht werden.

### Wie ist Privatsphäre im Bereich von Krypto-Währungen zu definieren?

Bevor auf die Erhaltung der Privatsphäre beim Traden mit Bitcoins eingegangen werden kann, muss zunächst die verwendete Definition geklärt werden: Im Folgenden wird unter Privatsphäre die Fähigkeit einer Person oder Gruppe verstanden sich selbst oder Informationen über sich selbst zu verstecken und sich dadurch auszudrücken, wie sie das will.

Konkret auf Geld bezogen ergeben sich daher zwei zentrale Komponenten der Privatsphäre: Anonymität und Transparenz. Das Zusammenspiel von Privatsphäre, Anonymität und Transparenz lässt sich durch die mathematische Formel $P = A / T$ ausdrücken. Folglich ist die Privatsphäre am höchsten, wenn die Anonymität am höchsten und die Transparenz am niedrigsten ist.

### Ist die Anonymität bei Online-Transaktionen mit Bitcoins gewährleistet?

Doch wann ist die Anonymität hoch und die Transparenz niedrig? Das etymologisch auf die alten Griechen zurückzuführende Wort „Anonymität" bezeichnet den Zustand ohne eigenen Namen oder die Namenlosigkeit. Auf Geld bezogen ist von vollständiger Anonymität zu sprechen, wenn niemand erkennen kann, wer sich hinter einer Kryptowährungs-Adresse verbirgt. Eine Blockchain nimmt keinerlei Unterscheidung zwischen Alter, Rasse, Herkunft, Geschlecht oder Bildung vor, weswegen Kryptowährungen zunächst hundertprozentige Anonymität hinsichtlich der Generierung eines zufälligen Privat Key zu gewähren scheinen.

Allerdings gibt es inzwischen zahlreiche durch Regierungen eingeführte Normenkomplexe, die illegale Aktivitäten durch Kryptowährungen verhindern sollen. So fordern Behörden inzwischen im Falle von Kryptowährungs-Exchanges eine Kontrolle im Rahmen von Anti-Geldwäsche-Systemen (Anti-Money-Laundering, AML) sowie der Terrorismusbekämpfung (Countering the Financing of Terrorism, CFL) und die Erhebung von Kundendaten (Know Your Customer, KYC und Know Your Business, KYB). Aus diesem Grund fordern die meisten Services einen Identitäts- und Altersnachweis als Voraussetzung des Tradens. Neben der Tatsache, dass die Anonymität durch Exchanges eine erhebliche Minderung erleidet, fällt auch noch eine andere Komponente ins Gewicht: Die Transparenz.

### Wie transparent sind Kryptowährungen?

Transparenz im sozioökonomischen Zusammenhang impliziert Offenheit, Kommunikation und Verantwortlichkeit. Kurz: Transparenz ist stets dann gegeben, wenn für Außenstehende erkennbar ist, welche Aktionen ausgeführt werden. Im finanziellen Kontext bedeutet das, dass die Wege der Geldflüsse bekannt sind. Im Bereich der Kryptowährungen stellt es sich so dar, dass der Großteil aller Blockchains über die gesamte Geschichte hinweg zu 100% transparent ist. Es gibt zwar neuere Technologien, die die Transparenz verringern sollen, doch im Grundsatz ist von vollständiger Transparenz bei Bitcoins auszugehen. Bezogen auf die oben aufgestellte Formel bedeutet das, dass sowohl Anonymität als auch Transparenz bei Kryptowährungen nahezu unendlich hoch sind. Dies führt zu einer Pseudo-Anonymität beim Handeln mit Kryptowährungen.

### Was ist unter Pseudo-Anonymität bei Krypto-Währungen zu verstehen?

Unter Pseudo-Anonymität im Bereich von Bitcoins ist zu verstehen, dass ein Computer trotz der hohen Transparenz dessen, was passiert, und trotz zunächst scheinbar hoher Anonymität Transaktionen unter Verwendung bestimmter Informationen zurückrechnen kann, die fehlende Informationen zu einer Identität zusammensetzen und somit die Anonymität reduzieren könnte. Selbst wenn die eigene Identität der Person im Rahmen der Transaktionen nie zum Vorschein kommt, ist auf diese Weise nachvollziehbar, welche Person hinter welchem Nutzer steht und wer beispielsweise ein bestimmtes Finanzverbrechen begangen hat. Dies hat in der Vergangenheit nicht nur theoretisch funktioniert, sondern wurde von Regierungen bereits mehrfach im Rahmen der Kriminalitätsbekämpfung angewandt.

So wurde der US-Amerikaner Ross Ulbricht im Jahr 2015 wegen Geldwäsche und Drogenhandel mit Kryptowährungen zu lebenslanger Haft verurteilt. Durch die Verwendung von Bitcoins als Zahlungsquelle hatten die Behörden Zugriff auf seine gesamte Transaktions-Historie. Als das Niveau an Anonymität bei einigen Transaktionen litt, konnten die Behörden ohne große Probleme seine Identität herausfinden und zugleich


Bild: iStock

aufgrund der Transparenz des Systems illegale Aktivitäten nachweisen. Es zeigt sich deutlich, dass das Level an Anonymität bei Kryptowährungen deutlich geringer ist, als bei der Verwendung von Bargeld oder anderen Fiat-Geldern.

### Wie kann die echte Anonymität bei Bitcoins erhöht werden?

Es gibt einige Technologien, welche die Anonymität beim Traden mit Bitcoins maximieren können. An dieser Stelle sind insbesondere Zero-Knowledge-Proofs und Ringsignaturen zu nennen.

Bei Zero-Knowledge-Proofs wird eine bestimmte Summe Bitcoins nur dann an einen Public Key übertragen, wenn der Inhaber dieses Public Key über eine bestimmte Information verfügt, die nur der berechtigte Empfänger kennt. So muss er seine Identität nicht offenlegen, sondern nur durch die entsprechende Information die Zahlung autorisieren. Bei Ringsignaturen handelt es sich um eine besondere, anonyme Form von Gruppensignaturen in kryptographischen Hash-Funktionen. Unter Zuhilfenahme einer Ring-Signatur kann der Nachweis erbracht werden, dass ein Gruppenmitglied ein bestimmtes Datum erzeugt hat, ohne dass das Gruppenmitglied seine Identität offenbaren muss.

### Wie hoch ist die Gefahr von Datendiebstahl und -missbrauch bei Bitcoins?

Eine Blockchain zu hacken ist im Moment absolut unmöglich. Dies würde nämlich bedeuten, die Kryptographie zu hacken. Diese kryptographischen Algorithmen wie SHA256 sind jedoch nicht kennzeichnend für die Blockchain, sondern werden überall im Internet verwendet. Ein solcher Hack würde die Welt also in ungeahnter Art und Weise treffen und massive Schäden anrichten. Es ist aber einfach nicht möglich, ausgehend von den Public Adresses die Private Keys zu ermitteln – genau das ist jedoch die Basis einer jeden Blockchain.

Vielmehr sind Pishing-Angriffe möglich. Diese sind vergleichbar mit dem Hack anderer Services, wenn Angreifer beispielsweise das Passwort für das Online-Banking ausfindig machen möchten. Fraglich ist also, ob es beim Traden mit Kryptowährungen leichter ist, Zugriff auf das „Konto" des Nutzers zu bekommen als bei klassischen Überweisungen. Bei einer normalen Überweisung benötigt der Hacker neben den Konto- und Zugangsdaten (PIN) inzwischen auch eine Transaktionsnummer (TAN), die meist auf ein mobiles Endgerät verschickt wird.

Bei der „Überweisung" von Bitcoins findet sich das Merkmal einer Kontonummer in Form des Public Key, die PIN in Gestalt des Private Key. Das Merkmal der TAN entfällt jedoch, da zwischen Empfänger und Begünstigtem keine Bank steht. Dies führt dazu, dass bereits die Kenntnis von Public und Private Key zu freier Verfügungsgewalt über das „Konto" des Betroffenen führt. Zudem folgt aus dem Fehlen einer Bank, dass der Public Key als Pendant zum Konto rechtlich keiner Person zugeordnet ist und das Konto folglich gläsern und für alle einsehbar im virtuellen Raum liegt.

### Welche Ansprüche hat der Geschädigte bei Datenmissbrauch?

Es wird angenommen, dass ein Hacker (Schädiger) den Private Key eines Nutzers (Geschädigter) erlangt hat und damit eine Überweisung auf ein von ihm genutztes Krypto-Konto tätigt. In dieser Konstellation sind die Rechte des Geschädigten nicht einfach zu beurteilen.

Denn ein Schutz des Geschädigten über §823 BGB ist nur schwer anzunehmen, da der „Diebstahl" eines Private Keys und die Übertragung der Bitcoins durch den Schädiger nur Teile der Rechnungseinheiten sind, während das Konto und der Schlüssel selbst jedoch nicht verloren gehen, sondern lediglich an Wert einbüßen. Das BGB kennt die Zuordnung von Rechtspositionen als Besitz oder Eigentum an einer Sache oder in Form der Inhaberschaft an Forderungen oder Rechten. Dieses System ist jedoch auf die oben aufgeführte Konstellation nicht ohne weiteres übertragbar. Denn Bitcoins und Kryptowährungen sind keine Sachen, da sie lediglich virtuell existieren. Entscheidend ist daher allein die Verfügungsgewalt über den Inhalt des „Kontos" in Form des Private Key. Im Gegensatz zum klassischen Konto ist der Public Key jedoch nicht mit einer konkreten Person verknüpft und insbesondere nicht mit dem Willen dieser Person verbunden. Es gibt nämlich keinen Kontoinhaber, nur faktisch auf das Konto Zugreifende.

Ein Anspruch des Geschädigten dürfte sich jedenfalls auf § 812 Abs. 1 Satz 1 2. Alt. BGB gründen lassen. Auf Basis einer Eingriffskondiktion kann der Geschädigte die übertragene Summe zurückfordern, wenn der Schädiger auf Kosten des Geschädigten ohne rechtlichen Grund etwas erlangt. Der Schädiger erlangt einen faktisch vermögenswerten Vorteil in Gestalt von Rechnungseinheiten, also ein adäquates Etwas. Dies geschieht auf Kosten des ursprünglichen alleinigen Kontoinhabers, des Geschädigten und ohne Rechtsgrund, da es sich ja um einen Hack handelt und eben nicht um eine normale Transaktion mit Leistung und Gegenleistung.

**Wo sind Bitcoins gesetzlich reguliert?**

Mit Geltung zum 01.01.2020 hat der deutsche Gesetzgeber einige Änderungen hinsichtlich Kryptowährungen vorgenommen. So hat er in Übererfüllung der 5. EU-Geldwäscherichtlinie das Kryptoverwahrungsgeschäft in § 1 Abs. 1a Nr. 6 Kreditwesengesetz (KWG) als Finanzdienstleistung aufgenommen und in § 1 Abs. 11 Nr. 10 Kryptowerte als Finanzinstrumente definiert. Unter Kryptowerten versteht der Gesetzgeber digitale Darstellungen eines Wertes, der von keiner Zentralbank oder öffentlichen Stelle emittiert wurde oder garantiert wird und nicht den gesetzlichen Status einer Währung oder von Geld besitzt, aber von natürlichen oder juristischen Personen aufgrund einer Vereinbarung oder tatsächlichen Übung als Tausch- oder Zahlungsmittel akzeptiert wird oder Anlagezwecken dient und der auf elektronischem Wege übertragen, gespeichert und gehandelt werden kann. Hierunter wird beispielsweise der Bitcoin verstanden.

**Was sind die Anforderungen an Bitcoin-bezogene Finanzinstrumente?**

Für Finanzdienstleistungen mit Bezug zu Kryptowährungen gelten zunächst die gleichen Anforderungen, die auch bei traditionellen Finanzinstrumenten berücksichtigt werden müssen. Wenn bspw. eine Anlageberatung stattfindet, bedarf es hierfür einer rechtlichen Erlaubnis zur Anlageberatung. Zusätzlich wird gefordert, dass den spezifischen, organisatorischen Anforderungen des entsprechenden Finanzdienstleistungsinstituts, welches die Dienstleistung im Zusammenhang mit Kryptowährungen anbietet, ausreichend Rechnung getragen wird. Insoweit müssen die Risiken aus den Geschäften mit den digitalen Finanzinstrumenten adäquat berücksichtigt werden. Das anbietende Finanzinstitut muss also insbesondere auch über die technisch-organisatorische Ausstattung für diese Art von Geschäften verfügen.

**Welche Anforderungen werden an das Kryptoverwahrungsgeschäft gestellt?**

Hohe praktische Relevanz hat die Neufassung des KWG aufgrund der Einführung des Kryptoverwahrungsgeschäfts. Da dieses als Finanzdienstleistungsinstitut eine Erlaubnispflicht auslöst, muss für die Verwahrung, Verwaltung und oder Sicherung von Kryptowerten – einschließlich dem Verwahren der kryptographischen Schlüssel – für andere eine Erlaubnis durch die BaFin eingeholt werden.

Diese Neuregelung hat insbesondere Einfluss auf die Kryptohandelsplattformen, soweit diese auch Verwahrung und Verwaltung der Token (also der Keys) anbieten. Hierbei spielt es insbesondere keine Rolle, welche Art von Verwahrung der jeweilige Betreiber anbietet. Denn neben den Wallets, die die Keys online zur Verfügung stellen, sind hiervon auch offline Wallets umfasst, die die Keys analog abspeichern. Anbieter, die allein die nötige Software und/oder Hardware zur Verfügung stellen, die eine Speicherung der Keys ermöglichen, sind jedoch keine Kryptoverwahrer, wenn sie keinen Zugriff auf die Keys erhalten.

Anbieter, deren Geschäftsmodell neuerdings unter eine Finanzdienstleistung fällt, müssen nunmehr die übliche Dokumentation implementieren und gegenüber der BaFin einreichen, die für die Erlaubnis einer jeden Finanzdienstleistung erforderlich ist (Organisationshandbuch, tragfähiger Geschäftsplan, Nachweis über Anfangskapital, Geschäftsleiterbeurteilungen, Angaben zu den Inhabern bedeutender Beteiligungen etc.). CRR-Kreditinstitute (sog. Vollbanken oder Universalbanken) hingegen benötigen keine separate Erlaubnis, da sie ohnehin sämtliche Finanzdienstleistungen erbringen dürfen.

Eine wichtige Änderung ist jedoch, dass Kryptoverwahrer nun geldwäscherechtlich Verpflichtete geworden sind und aus diesem Grund bei Geschäftsbegründung ihre Kunden identifizieren und die Angaben verifizieren müssen. Zudem bedarf es einer ständigen Überwachung der einzelnen Übertragungen (einschließlich der Übertragung von Kryptowährungen wie bspw. Bitcoins). Hierdurch werden die Trader einerseits aus ihrer Anonymität geholt und andererseits auffällige Transaktionen herausgefiltert. So sollen missbräuchliche Geschäfte (insbesondere Geldwäsche und Terrorismusfinanzierung) besser aufgespürt und verhindert werden können.

**Fazit**

Es wird deutlich, dass Kryptowährungen längst nicht das im Volksmund versprochene Maß an Anonymität bieten. Umfassende regulatorische Anforderungen, die durch die BaFin überwacht werden, sollen durch eine Absenkung des Anonymitätniveaus einem Missbrauch von Kryptowährungen Einhalt gebieten und spiegeln klar die Digitalstrategie der Bundesregierung wieder: Deutschland soll europäischer Vorreiter und Impulsgeber bei der Verbreitung von Kryptoassets werden.

Victor Masyula

# A case study on M-PESA as a form of e-payment

**What is M-PESA**

M-PESA ("M" for mobile and "PESA" for money in Swahili) is an electronic payment and electronic wallet system that is accessible through mobile phones. M-PESA, developed by mobile phone operator Vodafone and launched commercially by its Kenyan affiliate Safaricom in March 2007, is Africa's most successful mobile money service. It provides access to financial services to the millions of people who have a mobile phone, but do not have or have only limited access to a bank account. M-PESA

provides people with a safe, secure and affordable way to send and receive money, top-up airtime, make bill payments, receive salaries, get a short-term loan and much more. It has seen exceptional growth since its introduction by mobile phone operator Safaricom in Kenya.

**Introduction**

Payment is a pulse of any business, cash flow is considered as one of the critical success factors for any business as well as information and product flow. In this paper we will focus on one form of electronic payment used in Kenya known as M-PESA.

Electronic payment or e-payment is the payment of money for either goods or services without the physical exchange of hard cash.

**M-PESA in a Nutshell**

To access the service, customers must first register at an authorized M-PESA retail outlet. Their e-wallet account that is linked to their phone number's SIM card is activated. Customers can deposit to and withdraw cash from their e-wallets by exchanging cash for electronic value at a network of retail stores (often referred to as M-PESA agents). These M-PESA agents are paid a fee by Safaricom each time they exchange these two forms of liquidity on behalf of safaricom and its customers. Once customers have money in their M-PESA accounts, they can use their phones to transfer funds to other M-PESA users and even to non-registered users, pay bills, till numbers and purchase mobile airtime. All transactions are authorized and recorded in real time using secure SMS, and are capped at KES 100,000 (EUR 911). Customer registration and deposits are free. Customers then pay a small fee of between (KES 0 - KES 350/EUR 3.19) depending on the transaction amount, for person-to-person (P2P) transfers, bill payments and withdrawals. A fee of KES 10 / EUR 0.091 is charged for balance inquiries. Individual customer accounts are maintained in servers that are owned and managed by Safaricom. Safaricom deposits the full value of its customers' balances on the system in pooled accounts in two banks (CBA and KCB). Thus, Safaricom issues and manages the M-PESA accounts, but the value in the accounts is fully backed by highly liquid deposits at commercial banks. M-PESA is useful as a retail payment platform because it has extensive reach into large segments of the population. 98% of businesses in Kenya accept M-PESA.

**A simple User Interface**

The simplicity of M-PESA's message has been matched by the simplicity of its user interface. The M-PESA user interface is driven by an application that runs from the user's mobile phone. The service can be launched right from the phone's main menu, making it easy for users to find. The menu loads quickly because it resides on the phone and does not need to be downloaded from the network each time it is called. The menu prompts the user to provide the necessary information, one prompt at a time. For instance, for a P2P transfer, the user will be asked to enter the destination phone number, the amount of the transfer, and the personal identification number (PIN) of the sender. Once all the information is gathered, it is fed back to the customer for final confirmation. Once the customer hits ‚OK', it is sent to the M-PESA server in a single text message. Consolidating all information into a single message reduces messaging costs, as well as the risk of the transaction request being interrupted half-way through. A final advantage is that the application can use the security keys in the user's SIM card to encrypt messages end-to-end, from the user's handset to Safaricom's M-PESA server.




**M-PESA's Service Evolution**

M-PESA's original core offering was the P2P payment – enabling customers to send money to anyone with access to a mobile phone. It opened up a market for transactions which previously were handled largely informally – through personal trips, friends, and public transport networks. Many P2P transactions can be characterized as scheduled payments (such as sending a part of your salary to relatives back home), but many represent a basic form of finance, where people can draw on a much broader network of family members, friends, and business associates to access money as and when required.

Thus, M-PESA not only introduces a large measure of convenience to transactions that were already occurring, but it also enables a basic form of financial protection for a large number of users by enabling a network for instant, 'on demand' payments. In recent years, Safaricom has increasingly opened up M-PESA to institutional payments – enabling companies to pay salaries, collect bill payments and perform in-store purchases. Thus making M-PESA the market leader locally with more than 900 transactions per second.

The mobile financial services industry has grown significantly over the past ye-

ars since inception in 2007. The growth and viability of these services relies heavily on the existence of a payment platform that is convenient, easy to use, traceable and secure. The emergence of innovative mobile phone money transfers has put Kenya on the world's payment system map. It is notable that M-PESA has greatly enhanced access to financial services.

In particular, M-PESA has moved from the traditional role of transferring money to provision of banking services to both banked and unbanked. Commercial banks have partnered with Safaricom to enable customers to access their bank accounts through mobile phones. Mobile phones can be used for opening and operating virtual bank accounts (M-Shwari and KCB M-PESA) and access to traditional banking services like depositing, withdrawing and credit facilities without physical representation to the bank.

Of late they have now a loan and saving service right in M-PESA called M-Shwari.

**E-Payments in Kenya**

The last ten years has seen a steady rise in electronic payments in Kenya with banks, mobile operators and electronic payment firms focusing on the hundreds of thousands of small businesses in Kenya by introducing new products specifically aimed at paying for low-value transactions with ease, speed, and convenience. But the adoption of card-based (online & POS terminals) transactions in Kenya has been very slow. Most people don't trust electronic payments and some don't have bank accounts, people still believe in hard cash or cheque payments. Then came M-PESA which allowed even the unbanked population to start saving on their mobiles. This pushed mobile transactions as the mostly used form of e-payment in Kenya.

M-PESA can be credited with the steady rise of e-commerce businesses in Kenya, right now the local leader jumia.co.ke does 85% of its transactions via M-PESA. It is basically hustle-free online shopping, no credit cards, no bank details required. All the customer does at checkout is pay the shopping value to a particular merchant paybill number that will be displayed on the screen, and the customer will receive a confirmation message instantly, transaction done!

All major supermarkets and nearly all online shops in Kenya accept M-PESA payments via a paybill or till number.

Deutsche Übersetzung (durch die Redaktion)

# Eine Fallstudie zu M-PESA als einer Form der elektronischen Zahlung

**Was ist M-PESA?**

M-PESA („M" für Mobilgeräte und „PESA" für Geld auf Suaheli) ist ein elektronisches Zahlungs- sowie elektronisches Brieftaschensystem, das über Mobiltelefone zugänglich ist. M-PESA wurde von Vodafone entwickelt und im März 2007 in Kenia durch die Tochtergesellschaft Safaricom eingeführt und ist derzeit Afrikas erfolgreichster mobiler Gelddienst. Es bietet Zugang zu finanziellen Dienstleistungen für Millionen von Menschen, die zwar ein Mobiltelefon aber kein Bankkonto bzw. nur einen eingeschränkten Zugang auf ihr Bankkonto haben.

M-PESA bietet Menschen einen sicheren und erschwinglichen Weg Geld zu senden und zu empfangen. Sie können damit Mobilfunkgebühren aufladen, Rechnungen bezahlen, Gehälter empfangen, kurzfristige Darlehen erhalten und vieles mehr. M-PESA hat seit der Einführung in Kenia ein außergewöhnliches Wachstum verzeichnet.

**Einführung**

Bezahlung ist ein wichtiges Thema in jedem Unternehmen. Der Cashflow wird als einer der entscheidenden Erfolge angesehen, genauso wie der Informations- und Produktfluss. Dieser Artikel befasst sich mit der in Kenia verwendete Form der elektronischen Bezahlung, bekannt als M-PESA.

Elektronische Bezahlung oder E-Payment ist die Zahlung von Geld für Waren oder Dienstleistungen ohne den physischen Austausch von Bargeld.

**M-PESA auf den Punkt gebracht**

Um auf den Dienst zugreifen zu können, müssen sich Kunden zunächst in einem autorisierten M-PESA-Einzelhandelsgeschäft registrieren. Hierbei wird ein E-Wallet-Konto aktiviert, das mit der SIM-Karte verknüpft ist. Kunden können dann in verschieden Einzelhandelsgeschäften, die auch als M-PESA-Agenten bezeichnet werden, Bargeld auf das E-Wallet-Konto aufladen und auch abheben. Für jede dieser Transaktionen erhalten die M-PESA-Agenten eine Gebühr von Safaricom.

Sobald Kunden Guthaben auf ihren M-PESA-Konten haben, können sie mit Hilfe des Handys Geld mit anderen M-PESA-Nutzern austauschen und sogar Geld an nicht-M-PESA-Kunden überweisen, Rechnungen bezahlen und mobile Onlinezeit kaufen. Alle Transaktionen werden unter Verwendung von sicherer SMS-Technik autorisiert und in Echtzeit aufgezeichnet. Das Transaktionslimit beträgt 100.000 KES (ca. 911 Euro). Kundenregistrierung und Einzahlungen sind kostenlos. Ansonsten zahlen Kunden eine geringe Gebühr zwischen KES 0 und KES 350 (ca. 3,19 Euro), abhängig vom Transaktionsbetrag für direkte Überweisungen von einer Person zur anderen (P2P), Bezahlung von Rechnungen sowie Geld-Abhebungen. Für Kontostandsabfragen wird eine Gebühr von KES 10 (ca. 9 Cent) erhoben.

Die Kundenkonten werden auf Servern verwaltet, die Eigentum von Sa-

faricom sind und von Safaricom verwaltet werden.

Safaricom zahlt den vollen Wert der Guthaben seiner Kunden auf gepoolte Konten der Banken CBA und KCB ein. Somit gibt Safaricom zwar die M-PESA-Konten aus und verwaltet sie, aber das Guthaben der Konten ist vollständig durch hochliquide Einlagen bei Geschäftsbanken gedeckt.

M-PESA ist als Zahlungsplattform für Privatkunden nützlich, da es eine große Reichweite in der Bevölkerung hat. 98% der Unternehmen in Kenia akzeptieren M-PESA.

**Ein einfaches User-Interface**

Die Simplizität der M-PESA-Nachrichten wurde mit der Simplizität des User-Interfaces gepaart.

Das M-PESA-User-Interface ist eine Anwendung, die vom Mobiltelefon des Benutzers ausgeführt wird. Der Dienst kann direkt über das Hauptmenü des Telefons gestartet werden, so dass Benutzer ihn leicht finden können. Das Menü wird schnell geladen, da es sich auf dem Telefon befindet und nicht bei jedem Aufruf erst aus dem Netz heruntergeladen werden muss.

Das Menü führt die Nutzer Schritt für Schritt durch die Anwendung, um die notwendigen Informationen bereitzustellen. Zum Beispiel wird bei einer P2P-Überweisung die Telefonnummer des Empfängers, der Überweisungsbetrag und die persönliche Identifikationsnummer (PIN) des Senders abgefragt. Nachdem alle Informationen eingegeben wurden, erhält der Kunde eine Übersicht aller Informationen zur Prüfung und Bestätigung. Klickt der Kunde dann auf OK, werden die Daten per Textnachricht an den M-PESA-Server geschickt. Durch die Konsolidierung aller Informationen in einer einzigen Nachricht werden die Messaging-Kosten reduziert und das Risiko eingedämmt, dass die Transaktionsanforderung mitten drin unterbrochen wird. Ein letzter Vorteil ist, dass die Anwendung die Sicherheitsschlüssel auf der SIM-Karte des Benutzers verwenden kann, um Nachrichten Ende-zu-Ende zu verschlüsseln; also vom mobilen Gerät bis zum M-PESA-Server bei Safaricom.

**Service-Evolution von M-PESA**

Das ursprüngliche Kernangebot von M-PESA war das P2P-Payment, mit dem Kunden Geld an jeden senden können, der Zugang zu einem Mobiltelefon hat. So entstand ein Markt für Geldtransfers, der zuvor weitgehend informell gehandhabt wurde – durch persönliche Reisen, Freunde und öffentliche Verkehrsnetze. Viele P2P-Transaktionen können geplant und terminiert werden. Zum Beispiel das Senden eines Teils vom Gehalt an Verwandte zu Hause. Doch viele Dienste repräsentieren eine Grundform der Finanzierung, durch die Nutzer ein viel breiteres Netzwerk von Familienmitgliedern, Freunden und Geschäftspartnern haben, auf das sie bei Geldbedarf zurückgreifen können.

Somit bietet M-PESA nicht nur ein hohes Maß an Bequemlichkeit für Transaktionen, für die es ursprünglich gedacht war, sondern ermöglicht auch eine Grundform des finanziellen Schutzes für eine Vielzahl von Anwendern, indem ein Netzwerk von Diensten für On-Demand-Payment bereitgestellt wird. In den letzten Jahren hat Safaricom M-PESA mehr und mehr für institutionelle Zahlungen geöffnet, so dass Unternehmen Gehälter zahlen können, Rechnungen gesammelt gezahlt und Einkäufe in Geschäften durchgeführt werden können. Mit mehr als 900 Transaktionen pro Sekunde ist M-PESA der lokale Marktführer (Anmerkung der Redaktion: bezogen auf Kenia).

Die mobile Finanzdienstleistungsbranche ist in den letzten Jahren seit der Etablierung im Jahr 2007 erheblich gewachsen. Das Wachstum und die Rentabilität dieser Dienste hängen stark von der Existenz von Zahlungsplattformen ab, die bequem, benutzerfreundlich, rückverfolgbar und sicher sind. Dank der innovativen Entwicklung von Geldtransfers für Mobiltelefone wurde Kenia auf die Payment-System-Weltkarte gesetzt. Es ist bemerkenswert, dass M-PESA den Zugang zu Finanzdienstleistungen erheblich verbessert hat.

Insbesondere hat sich M-PESA von der traditionellen Rolle des Geldtransfers zur Bereitstellung von Bankdienstleistungen für Kunden mit oder ohne klassisches Konto entwickelt.

Bankgesellschaften haben mit Safaricom zusammengearbeitet, um Kunden den Zugriff auf ihre Bankkonten per Mobiltelefon zu ermöglichen. Handys können zur Eröffnung und zur Verwaltung virtueller Bankkonten von M-Shwari und KCB verwendet werden und ermöglichen so den Zugang zu traditionellen Bankdienstleistungen wie Einzahlungen, Abhebung und Überweisungen ohne eine Bank physisch aufsuchen zu müssen.

Neuerdings gibt es auch einen Kredit- und Sparservice in M-PESA. Der Dienst heißt M-Shwari.

**E-Payments in Kenia**

In den letzten zehn Jahren hat der elektronische Zahlungsverkehr in Kenia mit Banken, mobilen Anbietern und E-Payment-Firmen stetig zugenommen, die sich auf Hunderttausende kleine Unternehmen in Kenia konzentrieren und speziell darauf abzielen, durch die Einführung ihrer Produkte eine schnelle, einfache und unkomplizierte Bezahlmöglichkeit zu bieten.

Die Einführung von kartenbasierten Transaktionen, sowohl online als auch an POS-Terminals, war sehr langsam. Die meisten Menschen vertrauen elektronischer Bezahlung nicht und haben kein Bankkonto. Die Menschen glauben immer noch an Bargeld oder Schecks. Doch dann kam M-PESA, das es sogar der Bevölkerung ohne Bankkonten ermöglichte, per Handy mit dem Sparen zu beginnen. Das führte dazu, dass die mobile Transaktion in Kenia die am häufigsten verwendete Form des elektronischen Zahlungsverkehrs ist.

M-PESA kann der stetige Anstieg der E-Commerce-Unternehmen in Kenia zugeschrieben werden. Der lokale Marktführer jumia.co.ke führt 85% seiner Transaktionen über M-PESA durch. Es ist im Grunde genommen einfaches Online-Shopping, bei dem weder Kreditkarten noch Bankverbindung erforderlich ist. Alles, was der Kunde an der Kasse macht ist an eine bestimmte Händler-Rechnungsnummer zu bezahlen, die auf dem Display angezeigt wird. Der Kunde erhält postwendend eine Bestätigungsnachricht, dass die Transaktion abgeschlossen ist. Alle großen Supermärkte und fast alle Online-Shops in Kenia akzeptieren M-PESA-Bezahlung über Paybill oder Kassennummer.

Stephan A. Paxmann, Raik Borkowski

# PSD2 – Verbraucherschutz in einer digital vernetzten Gesellschaft

Stellen Sie sich vor, Ihnen wird in Ihrer Shopping App ein Fahrrad angezeigt, dass Ihr Interesse weckt. Stellen Sie sich dann vor, Sie können über die gleiche App Ihren Kontostand einsehen und überprüfen, ob Sie sich den Kauf des Fahrrads leisten können und wie die Zukunftsprognose Ihres Kontostandes aussieht, wenn Sie sich jetzt das Fahrrad kaufen. Stellen Sie sich vor, Ihre App zeigt Ihnen gleichzeitig an, welchen Ihrer sonstigen Verträge für Strom oder Versicherungen Sie bei welchem Anbieter günstiger abschließen können, sodass Sie Kosten einsparen und das gewünschte Fahrrad so finanzieren können. Und wenn Sie das Fahrrad sofort wollen, wird Ihnen ein Kredit zur direkten Echtzeit-Auszahlung angeboten, den Sie in der App in wenigen Minuten abschließen können. Auch die Zahlung können Sie unmittelbar aus Ihrer Shopping App heraus auslösen. Und nun stellen Sie sich vor, dass das alles möglich ist, ohne dass Sie sich ernsthaft Gedanken über den Missbrauch Ihrer Daten machen müssen.

Was wie ein Zukunftsszenario klingt, ist bereits heute möglich, und das seit dem 14. September 2019. Zu diesem Stichtag mussten offiziell alle Banken die Vorgaben der neuen Zahlungsrichtlinie PSD2 (Payment Service Directive) technisch umsetzen. Die Richtlinie schreibt Banken vor, sogenannten Drittanbietern, die nicht nur Banken oder Finanzdienstleister sein müssen, auf Kundenwunsch Zugang zu deren Kontodaten zu gewähren. Demnach ist eine direkte Interaktion zwischen dem Kunden und der Bank nicht mehr zwingend erforderlich. Kunden müssen beispielsweise bei der Abwicklung von Zahlungen nicht mehr zwingend auf ihr Bankkonto zugreifen, sondern können Drittanbieter dazu nutzen. Doch der Reihe nach.

### Einführung der ersten Zahlungsdiensterichtlinie PSD

In 2007 hatte die Europäische Union die Grundidee, einen einheitlichen Markt für Europas elektronische und nicht-elektronische Zahlungsdienste zu schaffen. Den gesetzlichen Rahmen für dieses Vorhaben sollte die erste Zahlungsdiensterichtlinie PSD stellen.

Ziel für die Zahlungsbranche war es, neben einer großen Auswahl an Zahlungsdienstleistungen für die Bürger der Europäischen Union (inklusive Norwegen, Island und Liechtenstein) den europäischen Wettbewerb durch die Teilnahme von Nicht-Banken zu verstärken. Dritte sollten vermehrt die Möglichkeit bekommen am Finanzsektor zu partizipieren und beispielsweise Finanzierungsdienste wie Lastschrift-, Überweisungs- und Zahlungskartentransfergeschäft anbieten zu dürfen.

Ziel in Bezug auf den Verbraucher war es, dessen Rechte zu erhöhen und schnellere Zahlungen zu garantieren. Denn gleichzeitig mit der PSD trat die Rechtsgrundlage für Europas Banken-Zahlungsinfrastruktur, besser bekannt als Single Euro Payment Area (SEPA) in Kraft. Mit ihr wurden Zahlungen für Verbraucher schneller und transparenter und brachten ein Anrecht auf Rückerstattungen mit sich.

Trotz der genannten Vorteile für europäische Händler und Endkonsumenten wurde das ambitionierte Ziel der PSD, eine größere Auswahl an Zahlungsdienstleistungen zu schaffen, nicht erreicht. Deshalb stellte die EU im Jahr 2013 den Antrag auf eine Neufassung der Zahlungsdiensterichtlinie und rief 2019 die PSD2 ins Leben.

### PSD2 nimmt den Verbraucherschutz stärker ins Visier

Die neue Zahlungsdiensterichtlinie PSD2 soll nicht nur die Entwicklung neuer, innovativer Bezahlarten, wie z.B. dem eWallet antreiben, sondern sie fasst auch den Datenschutz und die Sicherheit des Endnutzers bei elektronischen Zahlungen stärker ins Auge. So soll nicht nur die Sicherheit von Zahlungsdiensten erhöht werden, sondern auch der Verbraucherschutz bei Online-Zahlungen verbessert werden. Immer mit dem Ziel den digitalen europäischen Binnenmarkt so zu gestalten, dass er sowohl Verbrauchern als auch Unternehmen zugutekommt.

In diesem Sinne besteht das Regularium aus zwei wesentlichen Inhalten: der Zweifaktorauthentifizierung (2FA) und der Schnittstellenöffnung.

Die Zweifaktorauthentifizierung fokussiert die Sicherheit bei Online-Zahlungen. Demnach müssen sich Kunden seit dem 14. September 2019 bei der Abfrage ihrer Kontoinformationen sowie der Ausführung von Transaktionen zweifach authentifizieren. Diese Überprüfung erfolgt anhand einer Kombination der Elemente Wissen, Besitz und Biometrie. Üblicherweise wird hier neben den Login-Daten (Wissen) eine weitere Authentifizierung des Kunden verlangt, um den Zugriff auf dessen Bankkonto zu ermöglichen. Lästige Papier-Tans werden dabei entweder durch App-basierte Verfahren, physische Tan-Generatoren (Besitz) oder Fingerscans und Gesichtserkennung (Biometrie) ersetzt. Die Zweifaktorauthentifizierung soll Unbefugten den Zugriff auf das Bankkonto des Kunden deutlich erschweren bzw. unmöglich machen.

Die Schnittstellenöffnung oder Open Banking, wie es im Fachjargon heißt, ermöglicht es Drittdienstleistern, mit Zustimmung des Kunden Zugriff auf dessen Kontodaten zu erhalten. Um dies zu ermöglichen, müssen Banken ein Application Programming Interface (API), also eine einheitliche Programmierschnittstelle, bereitstellen. Auf dieser Basis kann jedes Unternehmen, das eine

Lizenz für die Erbringung von Finanzdienstleistungen besitzt, relevante Lösungen für Bankkunden entwickeln und sich an die Schnittstellen andocken.

Mit Hilfe dieser Kontozugänge soll ein Netzwerk aus bereits existierenden und neuen Lösungsanbietern entstehen. Hier kommen die so genannten Account Information Service Provider (AISPs) und Payment Initiation Service Provider (PISPs) ins Spiel.

**AISPs und PISPs**

Drittanbieter können im Rahmen der PSD2 als Kontoinformationsanbieter (AISP) oder Zahlungsauslöser (PISP) agieren.

Verfügt ein Kunde über mehr als ein Konto, besitzt er die Möglichkeit, einem AISP den Zugriff auf alle seine Konten zu gewähren, damit dieser die Informationen der verschiedenen Konten konsolidieren und analysieren kann. Der Kunde kann somit alle seine Transaktionen und Kontostände auf einer Oberfläche verwalten. Derartige Multibanking-Apps à la Finanzguru existierten zwar bereits vor der Einführung der PSD2, seit dem 14. September 2019 müssen sie sich aber an strenge regulatorische Anforderungen halten.

Darüber hinaus können Drittanbieter den Kunden auch als Zahlungsauslösedienste dienen. Die PISPs können im Kundenauftrag Zahlungen auslösen und bieten somit eine für den Kunden komfortable Alternative zur konventionellen Online-Zahlung per Kreditkarte. Dabei initiiert der PISP per Login in das Online Banking des Kunden eine Transaktion und löst die Überweisung in Echtzeit aus dem Kundenkonto der kontoführenden Bank aus.

Auch Zahlungsauslösedienste, wie das ursprünglich deutsche Unternehmen Sofortüberweisung, gab es bereits vor der Einführung der PSD2, jedoch ohne vollständig reguliert zu sein.

**Das Nutzerpotenzial für Unternehmen und Verbraucher**

Im Rahmen der PSD2 kann jedes Unternehmen unter gewissen Voraussetzungen als Drittanbieter agieren: u.a. FinTechs, BigTechs wie zum Beispiel Google, Amazon oder Apple aber auch Online Händler.

Letztere haben z.B. die Möglichkeit mittels eigener Zahlungsdienste wertvolle Informationen über das Kaufverhalten ihrer Kunden zu gewinnen. Ein bekanntes Beispiel ist der Online Händler Zalando, der mit der Zalando Payment GmbH bereits einen eigenen Zahlungsdienst etabliert hat. Basierend auf den analysierten Kundendaten können so gezielte Produktangebote an die Kunden adressiert werden. Dies hebt die Kundenbindung noch einmal auf ein anderes Niveau. Gleichzeitig können Online Händler schnellere Lieferzyklen einhalten, da Verzögerungen durch die Zahlungsabwicklung vermieden werden.

Auch für Banken bietet die PSD2 entscheidende Vorteile. Denn nicht nur die Konkurrenten der Banken, sondern auch die Finanzinstitute selbst erhalten mehr Informationen über ihre Kunden. Deren Konto- und Transaktionsdaten bei anderen Instituten sind dabei besonders wertvoll. Banken können z.B. Kreditzusagen verteilen, ohne die typischen papierhaften Gehaltsnachweise des Kreditanfragenden anzufordern. Mit Zustimmung des Anfragenden können sie auf das Gehaltskonto des Kunden bei einem anderen Institut zugreifen und eine direkte Prüfung anhand der Geldflüsse durchführen. Die Bearbeitung von Kreditanfragen wird so leichter, schneller und günstiger.

Aber natürlich birgt die PSD2 auch Risiken für die etablierten Finanzinstitute, da sie ihr Monopol auf die Kontodaten der Kunden aufgeben müssen. Als größte Konkurrenten werden in diesem Zusammenhang die BigTechs gesehen. Diese verfügen nicht nur über große Innovationsbudgets und technische Ressourcen, sondern im Gegensatz zu den FinTechs auch über eine enorme Kundenreichweite. Google und Apple sind bereits mit ihren Bezahllösungen GooglePay und ApplePay in den deutschen Zahlungsverkehr vorgedrungen. Weitere Lösungen werden folgen. In den USA vergibt Amazon unter dem Label „Amazon Lending" bereits Kredite, Facebook macht Überweisungen via WhatsApp möglich und Google plant für dieses Jahr eigene Girokonten einzuführen.

Wer von diesem Wettbewerb und dem Wettlauf um die Innovationen in der Finanzbranche profitiert, ist der Endverbraucher. Maßgeschneiderte Angebote, mehr Komfort beim Bezahlen, eine bessere User Experience, und natürlich eine höhere Sicherheit bei der Online-Bezahlung sollen dem einzelnen Kunden im Zuge der PSD2 geboten werden.

**Der Datenschutz spielt in der PSD2 eine wesentliche Rolle**

Insbesondere die Frage nach dem Datenschutzaspekt beschäftigt viele Verbraucher, schließlich kann nun theoretisch jeder fremde Anbieter Zugriff auf die eigenen Kontodaten bekommen, oder?

So einfach ist es dann doch nicht. Jeder Anbieter, ob Online Händler, FinTech oder Bank muss natürlich gewisse Spielregeln befolgen:

Erstens, es ist keinem Drittanbieter erlaubt, ob AISP oder PISP, die personenbezogenen Daten ohne die ausdrückliche Zustimmung des Nutzers abzurufen, zu verarbeiten oder zu speichern (gemäß Art. 94 II. PSD). Durch den Verweis auf die seit dem 25. Mai 2018 geltende Datenschutz-Grundverordnung (Art. 6 Abs. 1a; DSGVO) kann diese Einwilligung mündlich, schriftlich oder elektronisch erfolgen, muss jedoch ausdrücklich erbracht werden und darf sich nicht aus den Umständen ergeben. Eine Möglichkeit zur Einholung dieser Einwilligung ist die Datenschutzerklärung. Die PSD2 legt dabei in Verbindung mit der DSGVO großen Wert auf Transparenz und Verständlichkeit. Dem Kunden muss also in einfacher und verständlicher Sprache erklärt werden, wozu genau eingewilligt wird.

Zweitens, Drittdienstleister müssen den Grundsatz der Zweckbindung befolgen, welcher eine klare Zuordnung der Erhebung von Daten zu einem bestimmten Zweck erfordert, der bei der Erhebung deutlich erkennbar sein muss. Demnach dürfen AISPs und PISPs nur die Daten speichern, verarbeiten und nutzen, die für den vom Verbraucher erlaubten Zweck notwendig sind. Drittdienstleister dürfen die erhobenen Daten beispielsweise nicht ohne Einwilligung des Kunden für Werbung verwenden. Somit wird dem Risiko einer Zweckentfremdung der Kundendaten entgegengewirkt.

Drittens, Drittdienstleister müssen sowohl gegenüber Banken als auch ge-

genüber Betroffenen den Grundsatz der Datenminimierung (Art. 5 Abs. 1 c DSGVO) berücksichtigen, d.h. es dürfen nie mehr Daten erhoben werden, als für die Umsetzung des entsprechenden Kundenauftrages erforderlich sind. Demnach genügt es, wenn die Bank dem Zahlungsauslösedienstleister mitteilt, ob der angefragte Transaktionsbetrag verfügbar ist und entsprechend ausgezahlt wird. Dieser Grundsatz soll sicherstellen, dass Daten nicht unangemessen erhoben und verarbeitet werden.

Viertens, im Zuge der Produktentwicklung müssen Drittanbieter datenschutzrechtliche Voreinstellungen treffen (Privacy by Design & Privacy by Default), sodass während der gesamten Produktentwicklung der Schutz bezogener Daten bereits integriert ist. Demnach müssen Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen treffen, um dem Kunden ein angemessenes Schutzniveau zu gewährleisten (Art. 32 DSGVO). Damit soll die Verarbeitung personenbezogener Daten auf ein Minimum reduziert werden, was z.B. durch die Pseudonymisierung und Verschlüsselung personenbezogener Daten erfolgen kann.

Zu guter Letzt brauchen Drittanbieter eine Lizenz mit definierten Zugriffsberechtigungen, um die Schnittstellen der Banken nutzen zu können. Eine solche Lizenz vergibt die BaFin oder eine vergleichbare europäische Behörde. Somit ist die Befürchtung der Verbraucher, dass jeder Anbieter mit der Einführung der PSD2 Zugriff auf die Kontodaten erhält, unbegründet.

**Vernetzte Gesellschaft und Datenschutz – das kann funktionieren**

Es bestehen zahlreiche Vorteile der PSD2 für Banken, Drittanbieter und Endverbraucher, sodass wir dem Modell einer vernetzten Gesellschaft etwas nähergekommen sind. Zudem werden mit der PSD2 sowie der DSGVO auch sämtliche Aspekte des Verbraucherschutzes adressiert. Die Möglichkeit von Drittanbietern, sich via Schnittstelle Zugriff zu den Kunden- und Transaktionsdaten bei etablierten Banken zu verschaffen, mag Verbraucher auf den ersten Blick abschrecken, jedoch sind Befürchtungen eines Datenmissbrauchs unbegründet, da sich die Drittdienstleister an strenge Vorgaben halten müssen. Sollten sie diese nicht einhalten, droht ihnen eine Strafe von bis zu 20 Mio € oder 4% ihres Jahresumsatzes. Weiterhin bietet die Zweifaktorauthentifizierung den Bankkunden einen Sicherheitsstandard, der den Zugriff Unbefugter auf das Kundenkonto quasi unmöglich macht.

Trotz der erwähnten Vorteile ist das Potenzial der PSD2 noch lange nicht ausgeschöpft. Während sich Drittdienstleister mit den Anforderungen des Regulators arrangieren, nähern sich Banken der Ausschöpfung des Potenzials nur schwerfällig an. Die Verbraucher können sich hingegen auf weitere innovative Produkte am Finanzmarkt und sämtliche weiteren Benefits freuen.

Denn in naher Zukunft wird aus dem heute schon Möglichen Realität. Dann kann auch ich als Kunde den Erwerb meines Fahrrads und damit einhergehend sämtliche Finanzangelegenheiten bequem aus meiner Shopping App heraus managen, ohne mir dabei Gedanken über die Weitergabe meiner Daten machen zu müssen.

Reizvolle Aussichten auf dem Weg zu einer vollständig vernetzten Gesellschaft.

Dr. Susanne Holzgraefe

# Oyster Card, OV Chipkaart und MoBIB-Karte unter der Datenschutz-Lupe

Nutzung des öffentlichen Nahverkehrs, ohne lästiges Ticketziehen; eine Art Geldkarte, die im Vorfeld aufgeladen und von der am Fahrtende der entsprechende Betrag für die Fahrt abgezogen wird. „Pay As You Go“ (PAYG) nennen es die Briten.

London war hier mit der Oyster Card[1] der Vorreiter. Für eine Gebühr von £5 kann jeder, selbst Touristen, an den Schaltern in den Stationen der Londoner-U-Bahn (Tube) und an den Flughäfen eine Oyster Card bekommen. Vor dem ersten Fahrtantritt muss die Karte aufgeladen werden. Ist nicht mehr genügend Geld für eine Fahrt auf der Karte, verweigert das Schrankensystem in den Stationen den Zugang zum Bahnsteig. Überall in den Stationen finden sich Automaten, an denen das Guthaben der Karte eingesehen und die Karte entweder mit Bargeld oder per Giro- bzw. Kreditkarte aufgeladen werden kann. Die Oyster Card ist quasi lebenslang gültig. Wird sie doch zurückgegeben, wird das noch vorhandene Guthaben auf der Karte zurückerstattet.

Überall in den Stationen gibt es auf dem Weg zu den Bahnsteigen Schranken, die das Vorhalten der Oyster Card unumgänglich machen. Ist genügend Guthaben auf der Karte, öffnet sich die Schranke. Ist nicht mehr genügend Mindestguthaben für eine Fahrt auf der Karte, so teilt das die Schranke mit. Die Karte muss dann erst an einem der umstehenden Automaten in der Station aufgeladen werden. Nach Ende einer Fahrt ist die Karte erneut an der Schranke am Ausgang vorzuhalten. Es wird angezeigt, was die Fahrt gekostet hat und der Betrag von der Karte abgezogen. Danach öffnet sich die Schranke.

Abgerechnet wird also nur, wenn auch wirklich gefahren wurde: Pay As You Go – Zahle, wenn Du hinausgehst. Darüber hinaus können sogenannte Season-Tickets, z.B. Wochen- und Monatskarten

sowie Bus-Pässe auf die Oyster Card geladen werden.

Das Oyster-System wurde 2003 eingeführt und bereits zehn Jahre später waren 60 Millionen Karten im Umlauf.[2] Die Engländer waren damals nicht die einzigen, die ein Chipkarten-System für den öffentlichen Nahverkehr entwickelten. Die Niederländer führten 2005 in Rotterdam die OV Chipkaart ein. Seit 2012 gibt es die OV Chipkaart in den gesamten Niederlanden.[3] Auch Brüssel schloss sich dem Trend an und führte 2008 die MoBIB-Karte[4] ein. Für den Fahrgast sieht es auf den ersten Blick so aus, als seien die Systeme sehr ähnlich, doch sie unterscheiden sich in vielen kleinen Details.

Auch in Deutschland gibt es immer mal wieder Kommunen, die ein „à la Oyster"-System in Erwägung ziehen und sogar streckenweise testen.

Wie aber sieht das bei den drei Systemen aus London, den Niederlanden und Brüssel mit dem Datenschutz aus? Sind die Karten anonym oder personalisiert? Werden Fahrgäste ausreichend informiert? Wie transparent sind die Systeme? Wie freiwillig ist eine Registrierung der Karte? Fragen, die hier genauer unter die Lupe genommen werden.

## Anonymität

### Ist die Oyster Card anonym nutzbar?

Am Anfang ist sie in jedem Fall anonym. Wird sie tatsächlich nur als PAYG genutzt und stets mit Bargeld aufgefüllt, bleibt sie anonym.

Selbstverständlich lässt sich heutzutage die Oyster Card auch bargeldlos auffüllen. Hierbei lässt sich nachvollziehen, an welchem Automaten in welcher Station die Karte von wem aufgeladen wurde. Wobei das „von wem" die Person ist, deren bargeldlose Zahlungsmöglichkeit genutzt wurde. Das muss nicht die Person sein, die letztendlich die Oyster Card nutzt. Die Oyster Card kann genauso gut via Apple Pay der Freundin oder der Kreditkarte der Oma oder eine anderen dritten Person aufgeladen werden.

Immer wieder bin ich bei meinen Besuchen in London und bei meinen Recherchen zur Anonymität der Oyster Card auf Ratschläge gestoßen Bewegungsmuster zu verschleiern, indem mehrere Oyster Cards genutzt werden oder indem sich mehrere Personen zusammenschließen, die sich dann jeweils gegenseitig ihre Oyster Cards aufladen.

In der Datenschutzerklärung[5] des Transport for London (TfL) zur Oyster Card wird ausdrücklich darauf hingewiesen, dass die Privatheit der Reisenden sehr ernst genommen wird, und TfL daher sehr strenge Richtlinien, Prozesse und technische Messmethoden für die Zugangskontrolle hat. Insbesondere auch für die Daten von Bezahl-Karten. Hier hält sich TfL strikt an den Payment Card Industry Data Security Standard (PCI-DSS).

In der Datenschutzerklärung, aber auch an anderen Stellen der offiziellen Webseiten des TfL wird die anonyme Nutzung der Oyster Card als selbstverständlich hingenommen und lediglich faktisch darauf hingewiesen, dass bei Verlust der Karte das Guthaben sowie die Wochen- oder Monatskarten nicht erstattet werden können.

Als Service bietet TfL seinen Kunden an die Karte zu registrieren, damit sie bei Verlust gesperrt und eventuell noch vorhandene Guthaben erstattet werden können.

Weder innerhalb Londons vor Ort noch auf den Webseiten der TfL konnten bei den Recherchen ein aufdringliches Werben um eine Registrierung der Oyster Card festgestellt werden.

Beim Thema Kindertickets ist London sehr kompliziert. Kinder unter elf fahren in Begleitung eines Erwachsenen fahren kostenlos. Reisen vier Kinder allein, dann kostet es einmal den Erwachsenenpreis. So oder so lassen sich Oyster Cards mit dem „Young Person Discount" aufladen und es gibt auch Oyster Cards speziell für Studierende. Alles anonym, also übertragbar und auf Vertrauensbasis.

### Wie anonym ist die OV Chipkaart?

Auch die OV Chipkaart lässt sich laut den Webseiten zur anonymen Nutzung der OV Chipkaart anonym nutzen.[6] Hier wird lediglich sachlich darauf hingewiesen, dass eine anonym genutzte Karte übertragbar ist und bei Verlust nicht ersetzt werden kann. Ist die Karte wirklich anonym? Schon auf der Webseite wird darauf hingewiesen, dass es Kinder- oder Pendlerrabatte nur für personalisierte Karten gibt. Darüber hinaus wird auf der Seite darauf hingewiesen, unbedingt die Nummer der OV Chipkaart zu notieren, weil sie für Rückfragen benötigt wird. Inwieweit derartige Rückfragen anonym sind, wird nicht erläutert.

Die OV Chipkaart lässt sich zwar an jedem NS Ticket Automaten aufladen, aber leider lassen viele Automaten nur noch bargeldlose Bezahlung zu. Wie damit umgegangen wird, geht aus der Datenschutzerklärung[7] der Translink Systems B.V., die hinter der OV Chipkaart steckt, nicht hervor. Die vollständige Datenschutzerklärung ist zwar sowohl in niederländischer als auch in englischer Sprache verfügbar, aber sie muss erst von der Privacy-Seite heruntergeladen werden.

Es entsteht hier der Eindruck, als sei eine wirklich anonyme Nutzung der OV Chipkaart nicht gewünscht.

### Wie sieht das mit der Anonymität bei der MoBIB-Karte aus?

Die MoBIB-Basic-Karte[8] ist nicht namensgebunden. Auf der offiziellen Webseite zur MoBIB-Karte wird lediglich darauf hingewiesen, dass sie von mehreren Personen genutzt werden kann. Ist sie aber wirklich anonym?

Die MoBIB-Basic-Karte kann an den Verkaufsstellen der Transport En Commun (TEC) erworben werden. Eine Zahlung mit Bargeld ist möglich. Darüber hinaus ist sie über die Maatschappij voor het Intercommunaal Vervoer te Brussel (MIVB) / Société de transports intercommunaux de Bruxelles (STIB) erhältlich. Die MIVB/STIB verkauft sie in Kiosken und sogenannten Bootiks. Auch hier sollte die Zahlung mit Bargeld problemlos möglich sein.

Alle anderen Anbieter der MoBIB-Karte bieten die Karte nur personalisiert an.

Was genau alles auf die Karte geladen werden kann, hängt vom Anbieter ab. Genau wie in den Niederlanden ist das Angebot begrenzt und es gibt diverse Ticket-Angebote, die nur mit personalisierten Karten genutzt werden dürfen.

### Wie sieht es mit dem Aufladen der Karte aus?

Aufgeladen werden kann die Karte ebenfalls in den Verkaufsstellen, aber

auch an Automaten. Die Automaten in Brüssel lassen auch noch die Bezahlung mit Bargeld zu, so dass die MoBIB-Basic-Karte wirklich anonym genutzt werden kann.

Eine Firma namens BMC ist gemeinsam mit den vier Verkehrsbetrieben für die personenbezogenen Daten rund um die MoBIB-Karte verantwortlich. Die Datenschutzerklärung[9] ist in den drei Landessprachen, sowie in Englisch vorhanden. Allerdings wird hier in keiner Sprache darauf eingegangen, was mit den Daten passiert, die bei der bargeldlosen Bezahlung anfallen.

## Transparenz

Was genau passiert mit den personenbezogenen Daten, die die Verkehrsbetriebe erheben? Werden sie vertraulich behandelt? Wie transparent und gut verständlich ist erklärt, was mit den Daten passiert?

Artikel 12 DSGVO schreibt vor, dass die Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache sein müssen.

Vorbildlich sind hier die Londoner. Die Datenschutzerklärung zur Oyster Card ist übersichtlich strukturiert und sehr gut verständlich geschrieben; kurze, klare Sätze mit möglichst einfachen Worten.

Hier ist genau aufgelistet, welche personenbezogenen Daten anfallen und zwar so, dass der Karteninhaber sich hier zu seiner Person auch genau die Einzeldaten dahinter vorstellen kann. Es steht da zum Beispiel nicht einfach „Stammdaten“ sondern „Name, Adresse, E-Mail-Adresse, Telefonnummer“. Dadurch, dass hier selbst an das Passwort, die Informationen bei bargeldloser Bezahlung, Transaktionsdaten, Korrespondenz- und Serviceanfrage-Daten und einiges mehr gedacht wurde, erweckt die Liste den Eindruck, dass sie vollständig ist.

Bei der entsprechend Art. 13 DSGVO anzugebenden Rechtsgrundlage steht nicht einfach nur ein Hinweis auf die DSGVO, sondern es wurde nicht-juristisch klar verständlich erklärt, warum die Informationen erhoben werden.

*„… Bei Oyster Card gibt es eine Reihe dieser „rechtlichen Gründe“, auf die wir uns stützen:*

*Unsere gesetzlichen und öffentlichen Funktionen:*

*Um Aktivitäten zur Förderung sicherer, integrierter, effizienter und wirtschaftlicher Verkehrsmöglichkeiten und -dienste sowie die Umsetzung der Verkehrsstrategie des Bürgermeisters durchzuführen*

*Wo Sie TfL Ihre Zustimmung gegeben haben, zum Beispiel:*

*Wenn Sie sich für den Empfang von Marketingnachrichten oder In-App-Benachrichtigungen von uns entschieden haben oder wenn Sie das Contact Center gebeten haben, ein Problem oder eine Beschwerde für Sie zu lösen …“*

Zitat aus der Datenschutzerklärung zur Oyster Card (eigene Übersetzung).

Es wird ganz genau erklärt, wie TfL die personenbezogenen Daten erhält und wie sie verwendet werden.

Wenn die Person keine personenbezogenen Daten hinterlassen möchte, wird darauf hingewiesen, dass kein Online Account angelegt und bei Verlust der Karte das Guthaben nicht erstattet werden kann. Die Datenschutzerklärung weist ausserdem darauf hin, dass bei völliger Anonymität bestimmte Dienstleistungen, wie die Lösung bestimmter Beschwerden und Bedenken nur verzögert oder gar nicht durchgeführt werden können.

Die hier aufgelisteten Nachteile bei anonymer Nutzung sind alle logisch nachvollziehbar. Auch ein verloren gegangenes Papierticket wird in der Regel nicht ersetzt und Beschwerden, dass der Automat zu viele Münzen geschluckt oder zu wenig Wechselgeld herausgegeben hat, können auch bei einem Papierticket nur schwer bis gar nicht nachvollzogen werden.

Auch beim Thema Datenspeicherung ist TfL offen. Es wird detailliert aufgelistet, welche Daten wo und wie lange gespeichert werden. Teilweise ist sogar angegeben, warum die Daten aufgehoben werden.

TfL hat auch eine verständlich geschriebene, allgemeine Beschreibung zu technischen und organisatorischen Maßnahmen mit in die Datenschutzerklärung aufgenommen:

*„Wir nehmen die Privatsphäre unserer Kunden sehr ernst und es gibt eine Reihe zuverlässiger Richtlinien, Prozesse und technischer Maßnahmen, um den Zugriff auf und die Verwendung von persönlichen Informationen im Zusammenhang mit Oyster-Daten zu kontrollieren und zu schützen. Das schließt Zahlungskartendaten ein, die gemäß dem PCI-DSS (Payment Card Industry Data Security Standard) behandelt werden.*

*Jeder, der Zugriff auf personenbezogene Daten hat, die in den Systemen von TfL gespeichert sind, muss jährlich die Datenschutz- und Datensicherheitschulungen von TfL absolvieren.*

*Wir veröffentlichen auch Anleitungen zu den Schritten, die Sie zum Schutz Ihrer persönlichen Daten unternehmen können.“*

Zitat aus der Datenschutzerklärung zur Oyster Card (eigene Übersetzung).

Unter dem Punkt automatisierte Entscheidungsfindung und Profiling wird herausgestellt, dass die zu zahlenden Kosten bei Pay-As-You-Go-Fahrten automatisch ermittelt werden. Es wird darauf hingewiesen, dass Reisen automatisch anhand vorheriger Reisen vervollständigt werden, wenn die Karte nicht an beiden Enden der Fahrt gelesen wurde. Es wird automatisch Geld erstattet, wenn auf der Fahrt etwas Unvorhergesehenes passiert ist und so weiter.

Die Liste der automatischen Entscheidungsfindungen ist sehr gut durchdacht und erweckt den Eindruck, ziemlich vollständig zu sein.

TfL stellt auch präzise heraus, an wen die Daten für welche Zwecke weitergegeben werden. Eine Weitergabe zu Werbezwecken wird nicht erwähnt. Der gesamte Auftritt erweckt aber auch nicht den Eindruck, als würde TfL Daten zu Werbezwecken weiter vermarkten.

Herausgestellt wird in der Datenschutzerklärung jedoch, dass eine Weitergabe zu Forschungszwecken innerhalb Großbritanniens und den Vereinigten Staaten stattfindet. Hier wird darauf hingewiesen, dass die Daten vor der Weitergabe pseudonymisiert werden und es bei den weitergegebenen Daten in keinem Fall möglich ist, Einzelpersonen zu identifizieren.

Auch die Rechte der Betroffenen sind in klar verständlicher Sprache beschrieben. Es gibt noch eine weitere Seite, die genau beschreibt, wie Betroffene Zugang zu ihren Daten erhalten.

Zusammengefasst lässt sich sagen: TfL arbeitet sehr transparent.

Dass ihnen der Schutz der Privatheit wichtig ist und sie in keinem Fall das

Vertrauen der Kunden verletzen möchten, ist hier klar erkennbar.

### Wie ist das mit der Transparenz bei der OV Chipkaart?

Auf der Datenschutz-Seite der OV Chipkaart steht nicht sehr viel, aber es gibt einen Link zu einem PDF, das weitere Informationen enthält.

Auch hier ist anfänglich eine klar verständliche Sprache gewählt. Das PDF ist zwar in niederländischer und auch in englischer Sprache abrufbar, aber beim Lesen entsteht schnell der Eindruck, dass das Werk auf die Schnelle entstanden ist, weil der Gesetzgeber es fordert.

Es wird explizit herausgestellt, dass die Daten nicht zu Marketingzwecken genutzt werden.

Die Gesellschaft verarbeitet den Namen, die Adresse, ein Foto, das Geschlecht, das Geburtsdatum, Kontodaten, Username und E-Mail-Adresse. Auffällig ist, dass hier weder das Passwort für den Online-Account gelistet ist noch Informationen zu Kreditkarten, mit denen bezahlt wird. Auf der Karte selbst sollen dann neben der eindeutigen Kartennummer noch die letzten 10 Reisen, die erforderlichen Ticketinformationen sowie das Guthaben und noch einmal das Geburtsdatum gespeichert sein.

Wofür wird das Geschlecht, das Geburtsdatum und die Telefonnummer benötigt? Wofür die Kontodaten? Warum wird die Adresse erhoben und wofür braucht die Gesellschaft ein Foto?

Die Fragen werden in der Erklärung nicht beantwortet und auch die Rechtsgrundlagen für die Erhebungen und Verarbeitungen sind nicht erläutert.

Es wird herausgestellt, dass anonyme OV Chipkaarts völlig anonym sind. Da stellt sich spontan die Frage: „Und was ist mit Informationen zur Kreditkarte, mit der die Karte bezahlt bzw. aufgeladen wurde?“

Sofort im Nachgang wird dann auch schon erläutert, dass auch für die anonyme Karte personenbezogene Daten erhoben werden. Die Karte ist also nicht so anonym, wie sie beworben wird. Als Beispiel wird angeführt, dass bei der Auszahlung des Guthabens einer abgelaufenen Karte zwingend das Bankkonto benötigt wird, auf das das Geld überwiesen werden soll. Demnach ist eine Barauszahlung nicht möglich. Wird eine Rückerstattung per Formular beantragt, werden eine ganze Reihe von personenbezogenen Daten erhoben, für die wieder weder ein Grund noch eine Rechtsgrundlage angegeben ist.

Beim telefonischen Kundenservice werden bei anonymen Karten nur die Fragen ohne Zuordnung zur Person festgehalten. Es sei denn, es bedarf weiterer Rücksprachen, für die dann eine Telefonnummer oder eine E-Mail-Adresse angegeben werden muss. So weit, so gut, aber direkt danach steht, dass Telefongespräche grundsätzlich aufgezeichnet und drei Monate aufbewahrt werden. Das widerspricht eindeutig der vorherigen Aussage, dass der Kundenservice bei anonymen Karten lediglich die Fragen speichert.

### Zu Forschungszwecken werden personenbezogene Daten weitergegeben:

*„Die Öffentlichen Verkehrsunternehmen wollen sicherstellen, dass der öffentliche Verkehr so effizient und effektiv wie möglich ist. Aus diesem Grund haben sie ein Interesse daran, Einblicke in die Reisemuster von Reisenden zu erhalten. Diese Erkenntnis ist auch für Dritte wichtig, beispielsweise für Regierungen, die die Aufgabe des (öffentlichen) Verkehrs haben und sich für die Verbesserung der Dienstleistungen für Reisende einsetzen.“*

Und dann heisst es weiter:

*„Die öffentlichen Verkehrsunternehmen haben gemeinsam entschieden, welche personenbezogenen Daten verwendet werden dürfen und wie die personenbezogenen Daten verwendet werden dürfen. Wir bezeichnen das auch als Informationsmanagement. Die Vereinbarungen sind in einer Kooperationsvereinbarung zwischen den öffentlichen Verkehrsunternehmen festgelegt.“*

Zitat aus der Datenschutzerklärung zur OV Chipkaart (eigene Übersetzung).

Welche Daten jetzt genau weitergeleitet werden, geht aus der Datenschutzerklärung nicht hervor. Auch bedenklich ist, dass die Verkehrsunternehmen hier selbst entschieden haben, welche Daten sie nutzen dürfen, ohne detailliert zu erklären, warum sie das entscheiden dürfen.

Weiter wird erklärt, dass doch nur die Reisedaten verwendet werden und keine weiteren Daten zur Identifizierung von Einzelpersonen.

In einem Nebensatz wird dann noch darauf hingewiesen, dass gegen die Verwendung der Reisedaten formlos per E-Mail widersprochen werden kann.

Die Daten werden alle 18 Monate aufbewahrt. Warum, wieso und weshalb wird nicht erläutert.

Die Rechte der Betroffenen sind einfach nur aufgelistet und im Nachgang wird erklärt, dass für das Auskunftsrecht eine Pass- oder Ausweiskopie benötigt wird.

Zusammengefasst ist die Datenschutzerklärung zur OV Chipkaart an einigen Stellen widersprüchlich und nicht immer leicht verständlich geschrieben. Was mit Kreditkartendaten oder auch der Kopie des Passes passiert, ist überhaupt nicht erwähnt. Karten, die als anonym beworben werden, sind nicht anonym. Bemühungen hier wirklich das Vertrauen der Kunden zu stärken, konnten nicht erkannt werden. Kunden wissen auch nach Lesen des Dokumentes nur sehr wenig darüber, wie ihre Daten genau verarbeitet werden.

### Und die Transparenz bei MoBIB?

Es gibt zum einen die vier Verkehrsbetriebe, die für den öffentlichen Verkehr in Brüssel zuständig sind. Darüber hinaus gibt es noch eine Aktiengesellschaft namens BMC, die gemeinsam mit den vier Verkehrsbetrieben für die personenbezogenen Daten, die bei der MOBIB Karte verarbeitet werden, verantwortlich ist.

In der Datenschutzerklärung wird anfangs sofort darauf hingewiesen, dass die Unternehmen die Daten untereinander austauschen und verarbeiten. Welche Art von Daten und zu welchem Zweck der Verarbeitung wird nicht weiter erläutert. BMC schließt im Nachsatz jegliche Haftung für die Datenschutzerklärung sowie die Haftung für den Umgang der Daten bei den Verkehrsbetrieben aus.

Es ist verwirrend, dass sie nicht für ihre eigens erstellten Dokumente haften. Auch dass sie im ersten Satz auf die gemeinsame Verantwortung hinweisen und zwei Sätze später sich jeglicher Haf-

tung entziehen möchten, erweckt nicht wirklich Vertrauen.

Es gibt keine Verlinkung zu weiteren verpflichtenden Informationen entsprechend Art. 13 DSGVO der anderen Verantwortlichen.

*„Außerdem kann BMC auch personenbezogene Daten verarbeiten, die Sie BMC freiwillig zur Verfügung gestellt haben, wenn Sie sich an BMC oder den BMC-Datenschutzbeauftragten wenden."* Zitat aus der Datenschutzerklärung zur MoBIB-Karte.

Es fehlt die Auflistung, welche Art von personenbezogenen Daten verarbeitet werden. Die gesamte Datenerhebung soll auf Freiwilligkeit basieren, denn andere Rechtsgrundlagen sind anfangs nicht angegeben. Weiter unten im Dokument wird dann aber doch noch das öffentliche Interesse als Rechtsgrundlage erwähnt.

Es wird darauf aufmerksam gemacht, dass die Daten an Subunternehmen weitergegeben werden. Eine Liste der Subunternehmen ist nicht verlinkt. Es wird lediglich erläutert, dass es sich dabei um IT-Support, Hosting, Unterstützungsdienste sowie Anwendungsdienste zur Durchführung von Marketing und Datenanalyse handelt.

*„BMC hat alle notwendigen Maßnahmen ergriffen, um sicherzustellen, dass Ihre personenbezogenen Daten gemäß den Anforderungen der GDPR geschützt bleiben."* Zitat aus der Datenschutzerklärung zur MoBIB-Karte.

Der Satz erweckt den Eindruck, dass sie nur die wirklich notwendigen Maßnahmen ergriffen haben und nichts darüber Hinausgehende. Welche Maßnahmen genau ergriffen wurden, wird allerdings nicht erläutert.

*„Sollte BMC Ihre personenbezogenen Daten an eine andere natürliche oder juristische Person übermitteln, bittet BMC Sie um eine vorherige Genehmigung."* Zitat aus der Datenschutzerklärung zur MoBIB-Karte.

Da es keine Liste gibt, an wen die Daten weitergeleitet werden, ist hier die Frage, was bedeutet „andere Person"?

*„Benötigt BMC die personenbezogenen Daten nicht mehr für eine Verarbeitung, die eine längere Aufbewahrungsfrist erfordert (z. B. im Falle eines Rechtsstreits), bewahrt BMC die oben genannten personenbezogenen Daten für die Dauer der Gültigkeit der MoBIB-Karte verlängert um drei Jahre auf."* Zitat aus der Datenschutzerklärung zur MoBIB-Karte.

Die Gültigkeit der MoBIB-Karte beträgt fünf Jahre. Das bedeutet, sämtliche Daten werden mindestens acht Jahre aufbewahrt. Eine Rechtsgrundlage dafür wird nicht genannt.

*„Ihre personenbezogenen Daten können außerhalb Belgiens übermittelt und verarbeitet werden. Genauer gesagt befinden sich unsere Server in der Europäischen Union und einige unserer Dienstleister sind weltweit tätig.*

*BMC hat jedoch im Falle einer Übermittlung personenbezogener Daten in Länder außerhalb der Europäischen Union die notwendigen Schutzmaßnahmen ergriffen, um sicherzustellen, dass Ihre personenbezogenen Daten in Übereinstimmung mit dieser Erklärung zum Schutz personenbezogener Daten und der DSGVO geschützt werden."* Zitat aus der Datenschutzerklärung zur MoBIB-Karte.

Wie schon erwähnt, fehlt die Liste, an wen die Daten weitergegeben werden. Es geht auch nicht hervor, für welche Zwecke genau die Daten in Drittländer übermittelt werden. Ausländische Unternehmen sollen die Daten in Übereinstimmung mit der Information, die für die Betroffenen bestimmt ist, schützen? Das klingt, als läge hier ein Missverständnis vor.

Die Rechte der Betroffenen wurden alle aufgelistet und mit einem Satz erklärt. Allerdings wurde zum Beispiel beim Widerspruchsrecht und auch beim Recht auf Löschung nicht genauer beschrieben, bei welchen Verarbeitungsschritten überhaupt widersprochen werden kann und welche Daten auf Grund von gesetzlich vorgeschriebenen Aufbewahrungsfristen nicht gelöscht werden können.

Beim Recht auf Datenübertragbarkeit wurde aus dem im Gesetzestext stehenden „maschinenlesbar" das Wort „lesbar", was zur Verwirrung vorhandener Schnittstellen führen dürfte.

Auf automatische Entscheidungsfindungen und Profiling wird gar nicht eingegangen.

Zusammengefasst lässt sich sagen, dass eine wirkliche Transparenz bei der MoBIB-Karte nicht gegeben ist.

## Datenspeicherung

Oyster Card beschreibt sehr genau, welche Daten wie lange aufbewahrt werden. So werden zum Beispiel die reinen Bewegungsdaten für acht Wochen kartengebunden gespeichert. Die Frist von acht Wochen wird als angemessen angesehen, damit Kunden ihre Reisen überprüfen oder Anfragen stellen können (z.B. zu Rückerstattungszwecken). Nach acht Wochen werden die Daten von der Karte getrennt.

Informationen zu Kredit- und andere Zahlungskarten werden 18 Monate aufbewahrt.

Bei der OV Chipkaart werden alle Daten 18 Monate aufbewahrt. Hier wird nicht zwischen unterschiedlichen Datenkategorien unterschieden und es werden auch keine weiteren Gründe für die Aufbewahrung angegeben.

Bei der MOBIB Karte werden alle Daten mindestens acht Jahre gespeichert. Auch hier gibt es keinerlei Transparenz. Es wird dem Betroffenen weder eine Begründung noch eine Rechtsgrundlage für die lange Speicherung in der Datenschutzerklärung mitgeteilt.

## Freiwilligkeit

TfL bietet keine Preisrabatte für registrierte Karten. Die Registrierung der Oyster Card ist freiwillig. Der Vorteil ist, dass Karten bei Verlust gesperrt und Guthaben erstattet werden können.

Anders ist es bei der OV Chipkaart und der MoBIB-Karte. Rabatte werden nur für registrierte Karten gewährt. Dadurch ist die Freiwilligkeit der Registrierung natürlich auch nicht mehr wirklich freiwillig.

Auch in London gibt es zum Beispiel Ermäßigungen für Kinder und Jugendliche. London hat hier sogar ziemlich komplizierte Regelungen. Dennoch muss niemand eine Oyster Card für Kinder und Jugendliche registrieren. Es wird hier darauf vertraut, dass die Person, die derartige Tarife nutzen möchte, auch berechtigt ist, sie zu nutzen.

Das ist nicht anders als bei einem Papierticket für Kinder in Deutschland. Auch da ist es nicht erforderlich, Identifizierungsmerkmale des Kindes vor der Nutzung auf das Ticket des Kindes zu schreiben.

Sowohl in den Niederlanden als auch in Brüssel sind die Karten für Minderjährigen-Tarife zu registrieren.

Monats- und Wochenkarten dürfen in den Niederlanden und in Brüssel nur mit registrierten Karten genutzt werden. Verglichen mit den deutschen Papiertickets kommt es in Deutschland auf den Verkehrsbetrieb an. Während in Berlin Monats-Karten übertragbar und anonym sind, gibt es in NRW viele Städte, in denen Monatsticket zwangsweise personalisiert und nicht übertragbar sind.

In London sind derartige Tarife, die auf die Oyster Card geladen werden können, selbstverständlich jeweils von der Person nutzbar, die die Karte bei sich führt.

Das Problem der zwangsweise personalisierten Nutzung sind also die Tickettarife. Dass in Deutschland die Tickets für den öffentlichen Nahverkehr möglichst nicht personalisiert sein sollten, wird in NRW bereits seit einigen Jahren im diskutiert.

## Vertraulichkeit

Während die Londoner Verkehrsbetriebe TfL sehr viel Wert darauf legen, dass die Kunden ihnen vertrauen, erwecken die Niederländer und die Brüssler Verkehrsbetriebe eher den Eindruck, als läge ihnen nicht viel an der Gewinnung des Vertrauens ihrer Kunden.

TfL macht viel, um dem Kunden zu vermitteln, dass nur die wirklich erforderlichen Informationen erhoben und verarbeitet werden und die Daten bei ihnen wirklich sicher sind und sehr vertraulich behandelt werden.

Bei der Translink Gesellschaft, die für die OV Chipkaart verantwortlich ist, entsteht beim Lesen der Datenschutzerklärung der Eindruck, dass sie kein wirkliches Interesse daran hat die Betroffenen transparent zu informieren. Aussagen sind widersprüchlich, es wird mit Anonymität geworben, die aber bei genauerem Hinsehen nicht gewährleistet wird.

Bei der MoBIB-Karte ist keine wirkliche Transparenz erkennbar. Der Wirrwarr mit den vier Verkehrsbetrieben plus einer Aktiengesellschaft macht es für Betroffene noch schwieriger das Gefühl zu bekommen, dass die geforderten personenbezogenen Daten wirklich vertraulich behandelt werden.

## Fazit

Keine Papiertickets mehr im öffentlichen Nahverkehr ist eine schöne Idee. Der Londoner Vorreiter, die Oyster Card, gibt viel, damit die dabei anfallenden, personenbezogenen Daten bei ihnen sicher sind und streng vertraulich behandelt werden. Eine Registrierung der Karte ist freiwillig und hat den Vorteil, dass sie bei Verlust gesperrt und Guthaben ersetzt werden kann. Sämtliche Tarife sind nicht personalisiert und damit übertragbar nutzbar.

Die OV Chipaart aus den Niederlanden wie auch die MoBIB-Karte sammeln eine Reihe von Informationen ohne die Betroffenen genau über die Gründe und Rechtsgrundlagen dafür aufzuklären. Es entsteht der Eindruck, als sei Datenschutz für sie eher eine Last als ein Gewinn des Vertrauens der Kunden. In beiden Systemen gibt es eine Vielzahl von Tarifen, die nur personengebunden verkauft werden. Selbst Kindertarife sind nur personalisiert erhältlich.

Deutsche Verkehrsbetriebe, die über die Einführung eines ähnlichen Systems nachdenken, sind gut beraten, nicht die Niederlande oder Brüssel als Vorbild zu nehmen, sondern sich an den Londonern zu orientieren. Natürlich gibt es auch bei den Londonern noch Verbesserungspotential. Aber das wäre ja ein guter Ansporn für die Deutschen Verkehrsbetriebe, genau an den Stellen die Verbesserungen gleich mit zu berücksichtigen.

1 Offizielle Webseite des Transport for London: https://oyster.tfl.gov.uk/oyster/entry.do

2 BBC News Artikel vom 1. Juli 2013: https://www.bbc.com/news/uk-england-london-23120759

3 Artikel der OV in Nederland Community zur Erläuterung der OV Chipkaart: https://wiki.ovinnederland.nl/wiki/OV-chipkaart

4 Offizielle Webseite der MoBIB-Karte (viersprachig) https://mobib.be

5 Datenschutzerklärung des Transport for London zur Oyster Card https://tfl.gov.uk/corporate/privacy-and-cookies/oyster-card

6 Anonyme Nutzung der OV Chipkaart https://www.ov-chipkaart.nl/purchase-an-ov-chipkaart/anonymous-ov-chipkaart.htm

7 Datenschutz-Seite der OV Chipkaart https://www.ov-chipkaart.nl/privacy.htm

8 Offizielle Webseite zur MoBIB-Karte https://mobib.be/de.html

9 Datenschutzerklärung zur MoBIB-Karte in deutsch https://mobib.be/privacy_DE.html

Victor Masyula

# Data protection in Kenya and how it affects e-payments

## Introduction

In daily interactions, people give out a lot of their personal data knowingly or unknowingly. Take the example of apps on play store. Before you install it, it is a precondition to allow it access to your personal information e.g. contacts, sms, storage and more… . Usually, you have to accept the terms and conditions before you can access the app. Most people do not read the details but are quick to accept whatever terms and conditions offered.

Many times after downloading an app, you have no control of what it will use your data for. Under most of the terms and conditions, consent is given to the app to do many things with your data, including third party sharing.

A lot of personal data is given out during online activities. Third parties are able to access this information and use personal data for various purposes like marketing. Digitalisation has enhanced data exchange. Before accessing most services you are required to give out your personal data. This is where the problem starts…

A few months ago Kenya passed a data protection law whose foundation is the right to privacy. Article 31 of the Constitution gives citizens some level of data privacy in communications.

## The Data Protection Act

The Data Protection Act, however, comes in to provide a legal framework on personal data usage, especially on digital platforms. In 2018, the European Union passed the General Data Protection Regulations (GDPR) and the Kenyan data protection law is said to be GDPR compliant.

There are a lot of provisions in the law, which are important to read ahead of enforcing the law. The data protection laws will bring about several changes in the business environment. One is that almost all businesses will have to put in place structures and operations to ensure compliance.

Most businesses handle data. For example, when a client procures your services, you usually have a client database containing information about the client. Therefore, this law will be applicable to businesses that either control or process data like Safaricom.

As long as you are in direct control of another person's data then the law applies to you.

The law sets out several requirements that must be put in place when handling another's personal data and this includes processing and profiling. The data must be handled lawfully, accurately and the data subject's consent must be given before it is shared to third parties. In the case of a business, when a client gives you personal information, then you have an obligation to honour the law's provisions when interacting with that data.

For example, you cannot disclose their information to others without seeking consent. Structurally, the law requires controllers and processors to nominate data protection officers whose main duty is to ensure compliance with the law. This is especially so for businesses that are regulated and licensed by the government, for example banks.

Data sourced from Kenya is now safeguarded. This is crucial, especially in the wake of the Cambridge Analytica data scandal and the influence of the 2017 Kenyan elections.

There is a state agency that will deal with enforcement and overseeing protection in Kenya.

The impact of this law will take some time to be realised but it is prudent to prepare in advance.

## The role of the central bank of Kenya

The Central Bank of Kenya (CBK) issued a guideline on cybersecurity for Payment Service Providers (PSPs).

## The Guideline

Requires PSPs to maintain a cybersecurity programme with specified minimum standards designed to mitigate cyber risk in the payment system in Kenya and places the ultimate responsibility for compliance with this requirement on the board of directors and senior management of PSPs. This requirement is one of those additional responsibilities not set out in the earlier Guidance Note on Cybersecurity for commercial banks.

**The highlights of the specified minimum standards PSPs are now required to maintain to mitigate cyber risk in the payment system are as follows:**

### *Governance structure*

The Guideline has set out the various roles to be carried out by the board of directors and senior management of a PSP including, amongst others: overseeing the cultivation and promotion of an ethical governance, management culture and awareness – setting "the right tone from the top" and implementing the board-approved cybersecurity strategy, policy and framework, respectively.

All PSPs are required to have a Chief Information Security Office (CISO). The roles of the CISO include amongst others: developing and implementing the PSP's cybersecurity programme and enforcing the cybersecurity policy; and periodically reporting on the organisation's cybersecurity posture to senior management, board of directors and audit committee.

A PSP is limited to outsourcing only the operational security functions of the CISO, such as information security monitoring, testing and threat intelligence, and will be required to seek the prior approval of CBK.

### *Cybersecurity strategy, frameworks and policies*

Each PSP shall implement and maintain a written policy or policies for the

protection of its information systems and confidential information stored on those information systems.

The policy should address key cybersecurity issues including: information security; data governance and classification; business continuity and disaster recovery planning; resources, systems and network security; customer data privacy; vendor and third party service provider management; risk assessment and incident response.

***Risk management***

Each PSP shall conduct a periodic risk assessment of the PSP's information systems sufficient to inform the design of the cybersecurity programme as required under the Guideline, including the identification of critical cyber assets and revision of controls to respond to technological developments and evolving threats.

***Outsourcing***

PSPs are required to ensure that their third party service providers i.e. cloud service providers comply with legal and regulatory frameworks as well as international best practices.

The relationship should be governed by an outsourcing agreement in the nature of a clearly written contract, the nature and detail of which should be appropriate to the materiality of the outsourced activity in relation to the ongoing business of the PSP.

PSPs are required to notify CBK of the intention to outsource functions, services and infrastructures at least 30 days before such outsourcing agreements are executed.

***Regular independent assessment and testing***

PSPs are also required to carry out regular independent assessment and audit. To achieve this, the Guideline requires PSPs to incorporate qualified information and communication technology (ICT) auditors within their internal audit team.

**Effect on E-Payments in Kenya**

Privacy laws are more relevant today than ever before. With data crossing borders following the increased internet penetration and increased use of social media and other digital information platforms, it is becoming more important to ensure that personal data is protected, processed and used for the correct purpose.

Kenya has seen a steady rise in mobile banking and e-wallets in the last 10 years and that has come at a cost of data protection.

June last year, two Safaricom Employees were charged for trying to sell customer data from the company database to buyers on the black market. The end user was not protected by Law in that case, but currently a safaricom customer has the power to sue Safaricom.

It's very common in Kenya to get a random SMS from a betting company or any other marketing company and you wonder how they got your number. This is the pain that has been existing with customer data in Kenya, we hope this new law will protect the consumer.

We have seen a rise in loan lending apps that mine data from your phones and sell to the highest bidder. Payment apps and the likes will now have to comply with the new data laws which will see the common user more protected

This law will highly impact e-payments in a very positive way, now the public will do transactions more confidently knowing there is a law protecting them.

Deutsche Übersetzung (durch die Redaktion)

# Datenschutz in Kenia und wie er sich auf E-Payment auswirkt

**Einleitung**

Menschen geben im täglichen Leben viele ihrer persönlichen Daten wissentlich oder unwissentlich weiter.

Zum Beispiel ist es bei der Installation bestimmter Apps aus dem Play Store zwingend erforderlich den Zugriff auf persönliche Daten wie Kontakte, SMS, Speicher usw. zu erlauben. Auch ist zwingend erforderlich die Kenntnis über die Allgemeinen Geschäftsbedingungen zu bestätigen. Die meisten Menschen klicken und damit akzeptieren die Bedingungen schnell ohne sie genau zu lesen.

Ist die App erst einmal heruntergeladen, haben die Nutzer keine Kontrolle, wofür ihre Daten verwendet werden. In vielen Fällen wird der App die Zustimmung erteilt, viele Dinge mit den Daten anzustellen, einschließlich der Weitergabe an Dritte.

Bei Online-Aktivitäten werden viele personenbezogene Daten weitergegeben. Dritte können darauf zugreifen und die personenbezogenen Informationen für verschiedene Zwecke wie Marketing nutzen. Die Digitalisierung hat den Datenaustausch verstärkt.

Bevor Nutzer auf die meisten Dienste zugreifen können, müssen sie ihre persönlichen Daten zur Verfügung stellen. Und genau das ist das Problem …

Kenia hat vor einigen Monaten ein Datenschutzgesetz verabschiedet, dessen Grundlage das Recht auf Privatsphäre ist. Artikel 31 der Verfassung gibt den Bürgern ein gewisses Maß an Datenschutz in der Kommunikation.

**Das Datenschutzgesetz**

Das Datenschutzgesetz bietet einen rechtlichen Rahmen für die Nutzung personenbezogene Daten, insbesondere auf digitalen Plattformen. 2018 hat die Europäische Union die Datenschutz-Grundverordnung (DSGVO) verabschiedet und das kenianische Datenschutzgesetz soll konform dazu sein.

Es gibt viele Bestimmungen im Gesetz, die vor der Durchsetzung des Gesetzes vorausschauend zu lesen sind. Die Da-

tenschutzgesetze werden verschiedene Änderungen im Geschäftsumfeld mit sich bringen, so dass fast alle Unternehmen Strukturen und Maßnahmen einrichten müssen, um den Compliance-Anforderungen gerecht zu werden.

Die meisten Unternehmen verarbeiten Daten. Beispielsweise wird für die Erbringung von Dienstleistungen eine Kunden-Datenbank geführt, die Informationen über die Kunden enthält. Hier greift das Gesetz. Es gilt für Unternehmen, die wie Safaricom Daten kontrollieren und verarbeiten.

Sofern eine direkte Kontrolle über Informationen zu anderen Personen besteht, greift das Gesetz.

Das Gesetz legt mehrere Anforderungen fest, die beim Umgang mit personenbezogenen Daten erfüllt sein müssen. Dazu gehört neben der Verarbeitung auch die Profilerstellung. Die Daten müssen rechtmäßig und akkurat verarbeitet werden und die Weitergabe an Dritte bedarf der Zustimmung. Unternehmen haben die Pflicht, die Gesetze und Bestimmungen einzuhalten, wenn sie von den Kunden personenbezogene Daten erhalten, mit denen sie Interaktionen durchführen. Beispielsweise können sie die Informationen nicht ohne Zustimmung an andere weitergeben.

Strukturell schreibt das Gesetz vor, dass für die Verarbeitung Verantwortliche und Verarbeitende Datenschutzbeauftragte benennen müssen, deren Hauptaufgabe es ist, die Einhaltung des Gesetzes sicherzustellen. Das gilt insbesondere für Unternehmen, die von der Regierung reguliert und lizenziert werden, wie zum Beispiel Banken.

Daten aus Kenia sind jetzt geschützt. Das ist besonders nach dem Datenskandal von Cambridge Analytica und dessen Einfluss auf die Wahlen in Kenia im Jahr 2017 wichtig.

Es gibt eine staatliche Behörde, die sich mit der Durchsetzung und Überwachung des Schutzes in Kenia befassen wird. Es wird einige Zeit dauern, bis die Auswirkungen dieses Gesetzes erkannt werden. Es ist jedoch ratsam, sich im Voraus vorzubereiten.

**Die Rolle der Zentralbank von Kenia**

Die Zentralbank von Kenia (CBK) hat eine Richtlinie zur Cybersicherheit für Zahlungsdienstleister – englisch: Payment Service Provider (PSPs) – herausgegeben.

**Die Richtlinie**

Die Richtlinie erfordert, dass PSPs ein Cybersicherheitsprogramm mit festgelegten Mindeststandards entwickeln und aufrechterhalten, um das Cyber-Risiko im Zahlungsverkehr in Kenia einzudämmen sowie die ultimative Verantwortung für die Einhaltung der Anforderungen in der Geschäftsleitung der PSPs zu positionieren. Die Anforderung ist eine der zusätzlichen Verantwortlichkeiten, die im früheren Leitfaden der Cybersicherheit für Banken nicht vorkam.

**Nachfolgend die wichtigsten einzuhaltenden Anforderungen in den Mindeststandards für PSPs, um das Cyber-Risiko im Zahlungssystem zu verringern:**

***Führungsstruktur***

In der Richtlinie sind die verschiedenen Aufgaben der Geschäftsführung und der leitenden Angestellten von PSPs festgelegt; unter anderem: Die Einführung und Förderung einer moralisch einwandfreien Führungs- und Verwaltungskultur sowie die Sorgfaltspflicht - vorbildliches Verhalten der höchsten Ebenen beziehungsweise die Förderung der Umsetzung der von der Geschäftsführung genehmigter Cybersecurity-Strategien, -Richtlinien und -Rahmenbedingungen.

Alle PSPs müssen über einen Chief Information Security Officer (CISO) verfügen. Die Rollen des CISO besteht anderem aus der Entwicklung und Umsetzung des Cybersecurity-Programms des PSP sowie der Durchsetzung der Cybersecurity-Richtlinien und der regelmäßigen Berichterstattung über die Cybersicherheit im Unternehmen gegenüber der oberen Verwaltungsebene, der Geschäftsführung und dem Audit-Komitee.

Ein PSP darf nur die operationelle Sicherheitsfunktionen des CISO auslagern, wie zum Beispiel die Überwachung, das Überprüfen und nachrichtendienstliche Analysen. Dafür ist jedoch eine Genehmigung der CBK erforderlich.

**Cybersecurity-Strategie, Rahmenbedingungen und Richtlinien**

Jeder PSP muss eine oder mehrere Richtlinien zum Schutz seiner Informationssysteme sowie vertraulicher Informationen, die in seinen Systemen gespeichert werden, festlegen. Die Richtlinie sollte sich mit wichtigen Fragen der Cybersicherheit befassen. Unter anderem: Informationssicherheit, Datenführung und Klassifizierung, Geschäftsfortführung und Disaster-Recovery-Planung sowie Ressourcen-, System- und Netzwerksicherheit, Kundendatenschutz, Lieferanten- und Dienstleister-Verwaltung, Risikobewertung und die Reaktion auf Vorfälle.

***Risikoverwaltung***

Jeder PSP führt regelmäßig eine Risikobewertung seiner Informationssysteme durch, die darauf ausgelegt ist, die Verantwortlichen für die Gestaltung des Cybersecurity-Programms gemäß der Richtlinien zu informieren, einschließlich der Identifizierung kritischer Cyber-Aktivitäten und der Revision der Kontrollen von technologischen Entwicklung und sich daraus entfaltenden Bedrohungen.

***Outsourcing***

PSPs müssen sicherstellen, dass ihre Dienstleister – wie Cloud-Dienstanbieter – die gesetzlichen und regulatorischen Rahmenbedingungen sowie internationale Best-Practice-Lösungen einhalten.

Die Beziehung sollte durch eine Outsourcing-Vereinbarung in der Art eines schriftlichen Vertrages klar geregelt sein, der Art und Einzelheiten der ausgelagerten Tätigkeit in Beziehung zum PSP genau beschreibt.

PSPs müssen mind. 30 Tage vor Abschluss der Outsourcing-Vereinbarung die CBK über die Absicht informieren, Funktionen, Dienste und Dienstleistungen auszulagern.

***Regelmäßige unabhängige Bewertung und Überprüfung***

PSPs müssen außerdem regelmäßig unabhängige Bewertungen und Audits durchführen. Die Richtlinie gibt vor, dass sie hierfür für Informations- und Kommunikationstechnologien qualifizierte Auditoren in ihrem internen Revisionsteam einsetzen müssen.

### Auswirkungen auf E-Payment in Kenia

Datenschutzgesetze sind heute relevanter als je zuvor. Mit grenzüberschreitenden Daten durch die immer weitere Verbreitung des Internets und die verstärkte Nutzung sozialer Medien sowie anderer digitaler Informations-Plattformen wird es immer wichtiger sicherzustellen, dass personenbezogene Daten geschützt und nur zweckgebunden verarbeitetet werden.

Kenia hat in den letzten zehn Jahren einen stetigen Anstieg von Mobile Banking und E-Wallets verzeichnet, nicht immer war alles dabei datenschutzkonform.

Im Juni letzten Jahres wurden zwei Safaricom-Mitarbeiter angeklagt, weil sie versucht hatten, Kundendaten auf dem Schwarzmarkt zu verkaufen. Der Endkunde war in diesem Fall gesetzlich nicht geschützt. Aber jetzt hätte ein Kunde die Macht, Safaricom zu verklagen.

In Kenia ist es üblich, zufällige Werbe-SMS von Wett-Büros und jeder anderen Vermarktungsgesellschaft zu erhalten. Der Empfänger fragt sich, woher sie die Nummer kennen. Das ist ein Grundproblem im Umgang mit Kundendaten in Kenia. Es bleibt zu hoffen, dass das neue Gesetz den Verbraucher zukünftig besser schützt.

Es wurde ein erhöhter Anstieg von Kreditvergabe Apps festgestellt, die Handydaten abgreifen und höchstbietend verkaufen. E-Payment-Apps und dergleichen müssen nun die neuen Datenschutzgesetze einhalten. Dadurch wird der normale Nutzer besser geschützt.

Das Gesetz wird sich für die Nutzer sehr positiv auf E-Payments auswirken. Mit dem Wissen, dass es ein schützendes Gesetz gibt, können Transaktionen vertraulicher durchgeführt werden.

Maike Grahneis

# Erhebung von Kontaktdaten – Infektionsschutz und Datenschutz (Redaktionsschluss 31.07.2020)

Auf Grundlage gemeinsamer Beschlüsse haben Bund und Länder sukzessive die Lockerung der pandemiebedingten Einschränkungen vereinbart.[1] Aber Bundeskanzlerin Merkel erklärte nach den Bund-Länder-Gesprächen am 17. Juni 2020: *„Solange es kein Medikament und keinen Impfstoff gibt, müssen wir mit der Pandemie leben“*. Die Bundeskanzlerin und die Regierungschefinnen[2] und Regierungschefs der Länder verständigten sich darauf, dass Maßnahmen wie der Mindestabstand von 1,5 Meter, das Tragen eines Mund-Nasen-Schutzes in bestimmten öffentlichen Bereichen, verstärkte Hygienemaßnahmen und das Instrument der Kontaktbeschränkungen weiterhin gelten.[3]

Zur Eindämmung des Coronavirus SARS-CoV-2 ist die Durchbrechung von Infektionsketten ein wichtiger Baustein. Auch aus den Bund-Länder-Gesprächen heißt es, dass die schnelle und vollständige Kontaktnachverfolgung elementarer Bestandteil der gemeinsamen Öffnungsstrategie der Länder sei. Je effizienter sie funktioniere, desto schneller und wirksamer könne auf ein auftretendes Ausbruchsgeschehen reagiert werden. [4]

**Inwieweit die Erfassung von Kontaktdaten datenschutzrechtlich erlaubt/verpflichtend ist, richtet sich nach den vorherrschenden rechtlichen Bestimmungen. Es gilt die jeweiligen zu beachtenden regionalen bzw. lokalen Maßnahmen fortwährend im Blick zu behalten:**

Informationen zu den geltenden Regelungen der Bundesländer sind auf den jeweiligen Internetseiten der Landesregierungen zu finden – lokale Maßnahmen sind hingegen auf den Internetseiten von Gemeinden bzw. Städten einzusehen.[5] Die Website „LexCorona“ bietet eine gute Orientierung über die in Deutschland im Zusammenhang mit der Corona-Krise erlassenen Rechtsakte.[6]

### Kontaktdaten zur Nachverfolgbarkeit von Infektionsketten

Seit ein paar Monaten sind Betriebsinhaber in bestimmten Branchen bzw. Einrichtungen verpflichtet, Namen und Kontaktdaten ihrer Gäste zur behördlichen Nachverfolgbarkeit von Infektionsketten zu erheben, z.B. wenn diese die Einrichtungen/Geschäftsräume betreten oder an Veranstaltungen teilnehmen.

Im Hinblick auf die Pflicht und konkrete Ausgestaltung der Kontaktdatenerfassung ist dringend anzuraten, die jeweiligen regionalen und lokalen Bestimmungen in den Blick zu nehmen und fortwährend zu verfolgen.

Eine solche Pflicht zur Erfassung und Speicherung der Kontaktdaten anwesender Personen kann sich z.B. für Betriebsinhaber in Hamburg aufgrund der Hamburgischen SARS-CoV-2-Eindämmungsverordnung (nachfolgend „HmbSARS-CoV-2-EindämmungsVO“)[7] ergeben. Aus der HmbSARS-CoV-2-EindämmungsVO werden Bereiche wie

- Veranstaltungen
- Friseursalons
- Dienstleistungsbetriebe der Körperpflege
- Gaststätten und ähnliche Einrichtungen
- Übernachtungsangebote
- Freizeiteinrichtungen
- Theater, Opern, Konzerthäuser, Musiktheater, Kinos, Planetarien
- Bildungseinrichtungen und -angebote
- Sportanlagen und Sportbetrieb
- Schwimmbäder
- Spielbanken, Spielhallen, Wettvermittlungsstellen

- Trägerinnen und Träger der Jugendhilfe
- Krankenhäuser, Vorsorge- und Rehabilitationseinrichtungen u.ä.
- Einrichtungen der Eingliederungshilfe
- Seniorentreffpunkte und -gruppen[8]

verpflichtet.

Um weitere Beispiele der Bundesländer zu nennen: In Niedersachsen fußt eine Kontaktdatenerfassung landesrechtlich auf der geltenden „Niedersächsischen Verordnung zur Neuordnung der Maßnahmen gegen die Ausbreitung des Corona-Virus SARS-CoV-2 (Niedersächsische Corona-Verordnung)"[9] und z.B. in Nordrhein-Westfalen auf der geltenden „Verordnung zum Schutz vor Neuinfizierungen mit dem Coronavirus SARS-CoV-2 (Coronaschutzverordnung – CoronaSchVO NRW)".[10] Die weiteren Bundesländer haben ihrerseits Regelungen getroffen. Ggf. bestehen zudem lokale Rechtsakte, die es zu beachten gilt.

## Datenschutzrechtliche Rahmenbedingungen am Beispiel Hamburgs

Im Fall der HmbSARS-CoV-2-EindämmungsVO[11] sind Kontaktdaten unter Angabe des Datums und der Uhrzeit der Eintragung in Textform zu erfassen und vier Wochen aufzubewahren.[12] In der Hansestadt sind unter den Kontaktdaten im Einzelnen der Name, die Wohnanschrift und eine Telefonnummer zu verstehen, vgl. § 7 Abs. 1 Nr. 1 HmbSARS-CoV-2-EindämmungsVO. Nach Ablauf der Aufbewahrungsfrist sind die Aufzeichnungen der Kontaktdaten zu löschen oder zu vernichten. Weiter stellt die HmbSARS-CoV-2-EindämmungsVO ausdrücklich klar, dass bei der Erfassung der Kontaktdaten sicherzustellen ist, dass unbefugte Dritte keine Kenntnis von den Kontaktdaten erlangen können. Zudem ist die Verwendung der Kontaktdaten zu anderen als den in § 7 HmbSARS-CoV-2-EindämmungsVO genannten Zwecken sowie deren Weitergabe an unbefugte Dritte untersagt.[13] Vor diesem Hintergrund stellt der Hamburgische Datenschutzbeauftragte für den Datenschutz und Informationsfreiheit (HmbBfDI) auf seiner Website klar, dass derartige Listen, in denen solche Daten geführt werden, weder offen ausliegen noch für jedermann zugänglich sein dürfen: *„Oftmals ist es besser, die Daten zu jedem erfassten Besucher/Kunden auf einem gesonderten Blatt zu führen und danach sicher wegzuschließen, wenn sie nicht elektronisch geführt werden. Alternativ bietet es sich vielfach an, die Daten schon bei der Terminvereinbarung abzufragen. In gastronomischen Einrichtungen kann eine gemeinsame Liste pro Gästegruppe genutzt werden. Diese tragen sich dann alle auf die Liste ein, die auf dem gemeinsam genutzten Tisch liegt und das Personal entfernt sie, bevor die nachfolgende Gästegruppe den Tisch einnimmt."*[14]

Nach § 7 Abs. 2 HmbSARS-CoV-2-EindämmungsVO hat der zur Datenerhebung Verpflichtete Personen, die die Erhebung ihrer Kontaktdaten verweigern, von dem Besuch oder der Nutzung der Einrichtung, der Gewerberäume, der Geschäftsräume, der Gaststätte, des Beherbergungsbetriebes oder des Ladenlokals oder von der Teilnahme an der Veranstaltung auszuschließen.

Liegt nach Maßgabe der HmbSARS-CoV-2-EindämmungsVO die Verpflichtung zur Kontaktdatenerhebung vor, lässt sich die Datenverarbeitung auf Art. 6 Abs. 1 lit. c) DSGVO in Verbindung mit der jeweiligen Norm aus der Eindämmungsverordnung stützen. Die Verarbeitung der personenbezogenen Daten ist dann zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt.[15] Nach Ansicht des HmbBfDI soll die Erhebung von Namen und Kontaktdaten über die (oben aufgezählten) Bereiche hinaus allenfalls in Konstellationen zulässig sein, *„die ein besonders hohes Infektionsrisiko bergen"*.[16] In Konstellationen, in denen keine Rechtspflicht, keine längeren Gespräche und kein Kontakt zu Körperflüssigkeiten besteht, bestehe allerdings keine Befugnis zur Kontaktdatenerfassung. So scheide eine Kundenregistrierung im Einzelhandel, aber auch für den öffentlichen Nahverkehr aus, in dem Fahrgäste zwar gegebenenfalls nebeneinandersitzen, jedoch regelmäßig kein Austausch erfolge. Inhaber könnten aber eine freiwillige Registrierung anbieten, sodass sich die Datenverarbeitung auf eine Einwilligung gem. Art. 6 Abs. 1 lit. a) DSGVO stützen lassen kann, wenn diese auch diskriminierungsfrei abgelehnt werden kann. Besucher müssten also selbst bei Ablehnung der Registrierung das Geschäftsangebot nutzen können.[17]

Für die Einhaltung der datenschutzrechtlichen Regelungen sind jeweils die Betriebsinhaber verantwortlich. Die datenschutzrechtliche Verantwortlichkeit ist in Art. 4 Nr. 7 DSGVO definiert. Der Verantwortliche hat die erfassten Daten vor einem unbefugten Zugriff zu schützen und sicher aufzubewahren. Findet die Datenerfassung durch den Inhaber mit einer offenen, für alle sichtbar ausliegenden Liste (z.B. am Eingang/ Tresen/an der Theke) statt, so stellt dies einen Verstoß gegen die DSGVO dar.[18]

Die in der HmbSARS-CoV-2-EindämmungsVO enthaltenen Regelungen werden von einem Katalog an Ordnungswidrigkeitsverstößen[19] und Bußgeldregelsätzen[20] flankiert. Bei den Verstößen handelt es sich um Ordnungswidrigkeiten nach § 73 Abs. 1a Nr. 24 IfSG. Derartige Ordnungswidrigkeiten werden nach Angaben des HmbBfDI von der zuständigen Behörde (Gesundheitsbehörde) geahndet. Der HmbBfDI stellt zudem klar, dass die Polizei zuständig sei, wenn die sachlich zuständige Behörde nicht handeln könne, etwa am Wochenende oder bei Personalengpässen im Außendienst. Im Zusammenhang mit der HmbSARS-CoV-2-EindämmungsVO kontrolliere der HmbBfDI ausschließlich, ob sich die Inhaber an die „Regeln des Datenschutzrechts" halten.[21]

## Informationen über die Datenverarbeitung

Werden personenbezogene Daten bei der betroffenen Person erhoben, ist der Verantwortliche gem. Art. 13 DSGVO verpflichtet, der betroffenen Person Informationen über die Verarbeitung seiner Daten mitzuteilen. Vor dem Hintergrund müssen entsprechende Datenschutzhinweise nach Maßgabe des Art. 13 DSGVO an die Kunden bzw. Besucher erfolgen, deren Kontaktdaten erfasst werden. Um der Informationspflicht zu entsprechen, kann am Ort der Erhebung (z. B. im Empfangsbereich), ein Aushang angebracht oder ein Informationsblatt ausgelegt werden.[22] Die Datenschutzinformationen müssen also nicht jeder erfassten Person individuell ausgehändigt werden.[23]

Die Landesbeauftragte für den Datenschutz Niedersachsen (LfD Niedersachsen) gibt in diesem Zuge auch den Hinweis, dass bereits erteilte Informationen nach Art. 13 DSGVO, die bereits in der Einrichtung an die betroffene Person erteilt wurden, entsprechend um den neuen Zweck, die Rechtsgrundlage, die Speicherdauer und die Empfänger ergänzt werden können.[24]

Nach Maßgabe der niedersächsischen Regelungen zur Kontaktdatenerhebung und nach Angabe des LfD Niedersachsen müssen die Informationen folgendes beinhalten[25]:

- Den Namen und die Kontaktdaten des Verantwortlichen,
- die Kontaktdaten des Datenschutzbeauftragten (soweit vorhanden),
- die Zwecke, zu denen die personenbezogenen Daten verarbeitet werden sowie die Rechtsgrundlagen für die Verarbeitung,
- die Empfänger oder Kategorien von Empfängern (z.B. Gesundheitsamt, wenn eine Person sich im Nachhinein als infiziert herausstellen sollte),
- die Dauer der Speicherung,
- der Hinweis auf das Bestehen des Rechts auf Auskunft, auf Berichtigung und auf Beschwerde bei einer Aufsichtsbehörde[26] und
- der Hinweis, dass die betroffenen Personen nur die Dienstleistung in Anspruch nehmen bzw. die Einrichtung betreten können, soweit sie mit der Datenerfassung einverstanden sind.[27]

Teilweise bieten Aufsichtsbehörden auch Muster zur Kontaktdatenerfassung bzw. für Informationen nach Art. 13 DSGVO an.[28]

## Datenübermittlung auf Anfrage

Aus den jeweiligen Bestimmungen ergibt sich regelmäßig, dass die Kontaktdaten der zuständigen Behörde[29] auf Verlangen vorzulegen sein sollen, vgl. z.B. § 7 Abs. 1 Nr. 3 HmbSARS-CoV-2-EindämmungsVO. Die LfD Niedersachsen erklärt im Hinblick auf Niedersachsen, dass eine Übermittlung jedoch nur dann erfolgen sollte, wenn der Verpflichtete zur Vorlage schriftlich aufgefordert werde. Um der datenschutzrechtlichen Rechenschaftspflicht (vgl. Art. 5 Abs. 2 DSGVO) zu genügen, empfiehlt die Landesbeauftragte jede (Aufforderung zur) Übermittlung zu dokumentieren, um nachweisbar zu halten, welche Liste wann an wen wie übermittelt wurde. Zudem stellt die Aufsichtsbehörde klar, dass auch darauf zu achten sei, dass die erfassten Daten ausschließlich auf einem sicheren Übertragungsweg übermittelt werden. Hier nennt die LfD Niedersachsen den Postweg, die Übermittlung per Fax oder per Mail mit Ende-zu-Ende-Verschlüsselung.[30]


Bild: iStock

## Woher haben Sie meine Nummer? – die Kontaktdatenerfassung in der Stichprobenbetrachtung

Die Verarbeitung personenbezogener Daten und damit auch die Erhebung der Kontaktdaten unterliegt dem Zweckbindungsgrundsatz gem. Art. 5 Abs. 1 lit. b) DSGVO. Betreiber dürfen die Daten daher nicht zweckentfremden, etwa indem sie diese Daten nutzen, um den Erfassten Werbung zukommen zu lassen, oder um diese für etwaige Kundenansprache zu nutzen.[31] In den vergangenen Tagen häuft sich die Diskussion um den Rückgriff auf die Kontaktdaten zu anderen Zwecken.[32] Laut Pressemitteilung vom 24.06.2020 erreichen den HmbBfDI zahlreiche Beratungsanfragen, aber auch Beschwerden im Hinblick auf die Kontaktdatenerfassung: Teilweise sei verbreitete Praxis, offene Listen im Eingangsbereich auszulegen, sodass die Kontaktdaten für nachfolgende Gäste offenliegen. Ein derartiger Umgang macht die Daten daher besonders missbrauchsanfällig. So liege der Aufsichtsbehörde nach eigenen Angaben auch ein erster Hinweis vor, dass eine Kundin nach dem Besuch in einem Restaurant unter Verwendung ihrer erfassten Mobilfunknummer zu privaten Zwecken kontaktiert wurde.[33]

Um die Wirtschaft vor Ort zu beraten und zu sensibilisieren, hat der HmbBfDI im Juni eine Stichprobe von 100 Gewerbe- und Gaststättenbetrieben in Teilen Hamburgs durchgeführt, darunter 97 Restaurants, 2 Bäckereien und 1 Friseursalon. Im Ergebnis falle die Prüfung überwiegend *erfreulich* aus, da in den meisten geprüften Betrieben eine datenschutzkonforme Verarbeitung der Kontaktdaten stattfinde. Allerdings hätten rund 33 % der geprüften Betriebe Listen verwendet, die offen ausliegen und für jedermann zugänglich sind.[34]

## Fazit

Es bleibt abzuwarten, wie sich die Corona-Situation in der nächsten Zeit weiterentwickeln wird. Derzeit scheint sich schon eine zweite Infektionswelle anzudeuten. Es muss also davon ausgegangen werden, dass uns Regelungen zur Pandemiebekämpfung noch geraume Zeit beschäftigen werden. Ob und wie damit auch weiterhin eine Kontaktdatenerfassung einhergeht, wird sich zeigen. Inwieweit die Erfassung von Kontaktdaten datenschutzrechtlich vorgeschrieben ist, richtet sich nach den jeweils aktuell vorherrschenden rechtlichen Bestimmungen im Einzelfall.

1 Bundeszentrale für gesundheitliche Aufklärung (BZgA), Coronavirus, Sich und andere schützen, „Welche Regelungen gelten zur Zeit für das öffentliche Leben in Deutschland?“, Stand 18.06.2020, abrufbar unter: https://www.infektionsschutz.de/coronavirus/fragen-und-antworten/sich-und-andere-schuetzen.html, abgerufen am 26.07.2020, künftig zitiert mit BZgA, Welche Regelungen gelten zur Zeit?, En. 1.

2 Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

3 Die Bundesregierung, 17.06.2020, „Mindestabstand und Hygieneregeln gelten weiterhin“, abrufbar unter: https://www.bundesregierung.de/breg-de/themen/coronavirus/bund-laender-gespraech-1761456, abgerufen am 26.07.2020.

4 Beschluss „Bewältigung der Corona-Pandemie“, Besprechung der Bundeskanzlerin mit den Regierungschefinnen und Regierungschefs der Länder am 17. Juni 2020, abrufbar unter: https://www.bundesregierung.de/resource/blob/973812/1761548/94bdb647e1b03200d8430ee22e504ea9/2020-06-17-infektionen-data.pdf?download=1, abgerufen am 26.07.2020.

5 So jedenfalls BZgA, Welche Regelungen gelten zur Zeit?, En. 1.

6 LexCorona, abrufbar unter: https://lexcorona.de/doku.php, abgerufen am 26.07.2020.

7 Verordnung zur Eindämmung der Ausbreitung des Coronavirus SARS-CoV-2 in der Freien und Hansestadt Hamburg (Hamburgische SARS-CoV-2-Eindämmungsverordnung – HmbSARS-CoV-2-EindämmungsVO vom 30. Juni 2020 (gültig ab 15. Juli 2020), abrufbar unter: https://www.hamburg.de/verordnung, abgerufen am 26.07.2020.

8 Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI), Datenschutz in Zeiten von Covid-19, Stand 02. Juli 2020, abrufbar unter: https://datenschutz-hamburg.de/pages/corona-faq, abgerufen am 26.07.2020, künftig zitiert mit HmbBfDI, Covid-19, En. 8.

9 Niedersachsen, Vorschriften der Landesregierung, abrufbar unter: https://www.niedersachsen.de/Coronavirus/vorschriften-der-landesregierung-185856.html, abgerufen am 26.07.2020.

10 Die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW), 15.06.2020, Hinweise zur Erfassung von Kundenkontaktdaten zwecks Rückverfolgbarkeit von Infektionsketten in Zusammenhang mit dem Coronavirus SARS-CoV-2 unter Verweis auf die Website der Landesregierung Nordrhein-Westfalen: https://www.land.nrw/corona, abrufbar unter: https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/Corona-und-Datenschutz/Gastronomie-Hinweise.html, abgerufen am 26.07.2020, künftig zitiert mit LDI NRW, Hinweise zur Erfassung von Kontaktdaten, En. 10.

11 Vgl. En. 6.

12 Bitte beachten Sie die jeweils regionalen/lokalen Bestimmungen. Die Ausführungen der Passage betrachtet lediglich die Rechtslage nach Maßgabe der HmbSARS-CoV-2-EindämmungsVO. In Niedersachsen (Niedersächsische Verordnung zur Neuordnung der Maßnahmen gegen die Ausbreitung des Corona-Virus SARS-CoV-2 (Niedersächsische Corona-Verordnung) vom 10. Juli 2020 (CoronaVO)) ergibt sich eine Pflicht zur Aufbewahrung für die Dauer von drei Wochen nach dem Ende des jeweiligen Ereignisses, vgl. § 4 S. 1 CoronaVO. § 4 S. 5 CoronaVO schreibt vor, dass die Kontaktdaten spätestens einen Monat nach dem Ende des jeweiligen Ereignisses zu löschen sind.

13 § 7 Abs. 1 Nr. 5 HmbSARS-CoV-2-EindämmungsVO; zur Lage in Niedersachsen: Die Landesbeauftragte für den Datenschutz in Niedersachsen (LfD Niedersachsen), Datenschutzkonforme Dokumentation zur Umsetzung der Niedersächsischen Verordnung zur Neuordnung der Maßnahmen gegen die Ausbreitung des Corona-Virus SARS-CoV-2, Stand: 13.07.2020, abrufbar unter: https://lfd.niedersachsen.de/startseite/themen/wirtschaft/corona-kontakdaten-187846.html, abgerufen am 26.07.2020, künftig zitiert mit LfD Niedersachsen, Niedersächsische Verordnung, En. 13.

14 HmbBfDI, Covid-19, En. 8.

15 Vgl auch HmbBfDI, Covid-19, En. 8, vgl. HmbBfDI, Mustervorlage Kontaktdatenerhebung, abrufbar unter: https://datenschutz-hamburg.de/assets/pdf/Mustervorlage_zur_Erfassung_von_Kontaktdaten.pdf., abgerufen am 26.07.2020, künftig zitiert mit HmbBfDI, Mustervorlage Kontaktdatenerhebung, En. 15.

16 Dazu im Einzelnen HmbBfDI, Covid-19, En. 8 unter Verweis auf Empfehlungen des Robert-Koch-Instituts.

17 HmbBfDI, Covid-19, En. 8.

18 HmbBfDI, Covid-19, En. 8.

19 vgl. § 39 HmbSARS-CoV-2-EindämmungsVO vom 30. Juni 2020 (gültig ab 15. Juli 2020).

20 hamburg.de, Bußgeldkatalog zur SARS-CoV-2-Eindämmungsverordnung, abrufbar unter: https://www.hamburg.de/bussgeldkatalog/, abgerufen am 26.07.2020.

21 HmbBfDI, Covid-19, En. 8.

22 LfD Niedersachsen, Niedersächsische Verordnung, En. 13.; für die Möglichkeit des Ausliegens oder Aushängens auch HmbBfDI, Covid-19, En. 8.

23 HmbBfDI, Covid-19, En. 8.

24 Vgl. LfD Niedersachsen, Niedersächsische Verordnung, En. 13.

25 So LfD Niedersachsen, Niedersächsische Verordnung, En. 13.

26 Das Muster des HmbBfDI (siehe En. 27) weist überdies darauf hin, dass der betroffenen Person „(...) sämtliche Betroffenenrechte nach Art. 15 ff. DSGVO, insbesondere Auskunft, Löschung, Einschränkung der Verarbeitung“ zustehen.

27 Zur Versagung des Zutritts in Hamburg vgl. § 7 Abs. 2 HmbSARS-CoV-2-EindämmungsVO.

28 Z.B. HmbBfDI, Mustervorlage Kontaktdatenerhebung, En.15; LfD Niedersachsen, Niedersächsische Verordnung, En. 13 unter „Muster zur Erfüllung der Informationspflichten während der Corona-Pandemie“.

29 Z.B. im Fall der HmbSARS-CoV-2-EindämmungsVO ist dies nach Ansicht des HmbBfDI die „Gesundheitsbehörde“: vgl. HmbBfDI, Mustervorlage Kontaktdatenerhebung, En. 15.

30 LfD Niedersachsen, Niedersächsische Verordnung, En. 13.

31 LDI NRW, Hinweise zur Erfassung von Kontaktdaten, En. 10; LfD Niedersachsen, Niedersächsische Verordnung, En. 13; vgl. HmbBfDI, Mustervorlage Kontaktdatenerhebung, En. 15.

32 n-tv, 06.07.2020, „Ungewollte Nachricht vom Kellner Corona-Listen werden immer wieder missbraucht“, abrufbar unter: https://www.n-tv.de/mediathek/videos/panorama/Corona-Listen-werden-immer-wieder-missbraucht-article21892388.html, abgerufen am 26.07.2020; zum polizeilichen Zugriff auf Kontaktdaten: Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz (LfDI), Pressemitteilung von 22.07.2020, „Polizei sollte auf Corona-Gästelisten nur mit richterlichem Beschluss zugreifen - Kugelmann: Es muss eine hohe Hürde geben“, abrufbar unter: https://www.datenschutz.rlp.de/de/aktuelles/detail/news/detail/News/polizei-sollte-auf-corona-gaestelisten-nur-mit-richterlichem-beschluss-zugreifen-kugelmann-es-muss/, abgerufen am 26.07.2020.

33 HmbBfDI, Datenschutz und Infektionsschutz gehen Hand in Hand, Pressemitteilung, 24.06.2020, abrufbar unter: https://datenschutz-hamburg.de/pressemitteilungen/2020/06/2020-06-24-kontaktdatenerfassung-stichprobe, abgerufen am: 26.07.2020, künftig zitiert mit HmbBfDI, Pressemitteilung 24.06.2020, En. 33.

34 HmbBfDI, Pressemitteilung 24.06.2020, En. 33.

Heinz Alenfelder

# Eine App, die zu viel kostet

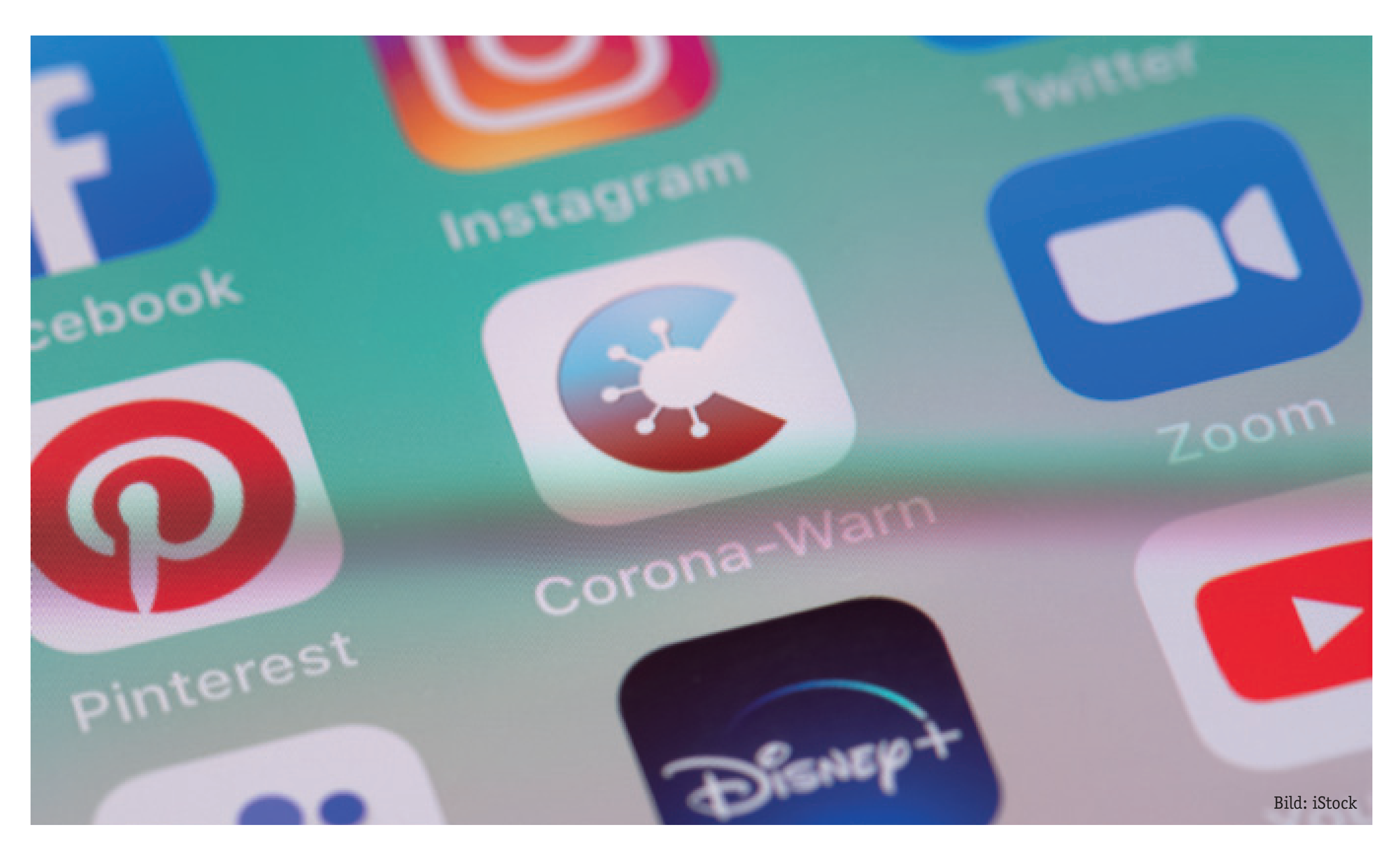



Bild: iStock

Die Corona-App kostet 20 Millionen Euro und funktioniert endlich. Zwar ist sie datenschutzkonform, doch der Preis ist zu hoch. Einen Nutzen hat die Entwicklung der Corona-App ja nun doch: Sie hat den Datenschutz von Smartphone-Apps generell zum Thema gemacht und auch dazu geführt, dass über datenschutzkonforme Lösungen auf den Mobilgeräten überhaupt ernsthaft diskutiert wird.

Bisher ist es vielfach so, dass bei Applikationen auf einem mobilen Telefon die „Datenschutzerklärung" – wenn überhaupt vorhanden – bestätigend weggeklickt wird und der App – je nach ihrem Zweck – der Zugriff auf Kontakte, Geopositionen, Gesprächsdaten usw. in der Regel gewährt wird. Wer dies verweigert, ist für die App-Industrie vernachlässigbar, da zu vermuten ist, dass diese „Außenseiter" gegebenenfalls gar nicht auf Werbeangebote reagiert hätten.

Bei der Entwicklung der aktuellen Corona-App änderten sich grundlegend einige Voraussetzungen: Einerseits wollen die Nutzenden wissen, wie die App funktioniert. Sie soll eben nicht alle Bewegungsdaten komplett erfassen und auch nicht registrieren, mit wem ich mich wann wo aufgehalten habe. Andererseits soll die App möglichst auf allen Mobilgeräten installiert sein.

Gesundheitsexperten gehen davon aus, dass die Unterbrechung von Infektionsketten per App erst bei einer Abdeckung von mehr als 60 Prozent in der Bevölkerung zum Eindämmen der Pandemie erfolgreich ist. Außerdem mussten die Mobilgiganten Apple und Google Schnittstellen programmieren, damit das Konzept umgesetzt werden konnte. Allein für die Entwicklung durch SAP und Telekom standen 20 Millionen Euro zur Verfügung. Betrieb und Wartung ziehen weitere Kosten in Millionenhöhe nach sich.

Im Fazit bleibt eine große Unzufriedenheit zurück, ist doch die Corona-App mit deutlicher Verspätung zur Verfügung gestellt worden und hatte anfangs massive Fehler. Hinzu kommt, dass Apple und Google die Schnittstellen offenlegen müssten, um kontrollieren zu können, was dort mit den Daten passiert. Natürlich handelt es sich aus Sicht des Datenschutzes bei den offen gelegten Teilen der App und der Art und Weise der Problemlösung um ein Modell, das hilft, personenbezogene Daten zu schützen. Dies allerdings hätte man sicher für weniger Geld haben können! (Eine App, die zu viel kostet, www.mittelbayerische.de 19.08.2020).



Foto: Heinz Alenfelder/Christiane Wittich

Maike Grahneis

# Die Corona-Warn-App – Nutzung im Beschäftigungsverhältnis

**Wenn die unternehmerische Existenz bedroht ist**

Seit ein paar Monaten stellt SARS-CoV-2, das sog. Corona-Virus, auch die Wirtschaft vor beispiellose Herausforderungen – viele Arbeitgeberinnen[1] und Arbeitgeber fürchten um ihr Geschäft, wenn nicht sogar um ihre Existenz. Mit milliardenschweren Hilfsprogrammen, Kurzarbeitergeld, steuerlichen Maßnahmen und einem gemeinsamen europäischen Krisenmanagement versucht man der Lage Herr zu werden und die Wirtschaft sukzessive zu stabilisieren.[2] Die Angst vor einer weiteren Infektionswelle ist hoch. Weiterhin gilt es, Infektionen zu vermeiden und die Gesundheit der Beschäftigten zu schützen. Einmal mehr wurde die Dringlichkeit, die hinter der Bekämpfung von Infektionsketten steckt, im Zuge der Berichterstattung zum Kreis Gütersloh im Juli präsent. Arbeitgeber sind daher nicht nur im eigenen Interesse gehalten, Schutzmaßnahmen einzuführen. Da kommt die Corona-Warn-App (CWA) doch auch gerade passend für das Arbeitsverhältnis – oder?

Dieser Artikel soll für ausgewählte arbeits- und datenschutzrechtliche Fragestellungen sensibilisieren, die mit dem Einsatz der Corona-Warn-App einhergehen. Dazu wird zunächst auf die Funktionsweise der App eingegangen. Sodann werden wesentliche Aspekte der Datenverarbeitung dargestellt, z.B. wer für die Datenverarbeitung im Rahmen der App verantwortlich ist, auf welcher Rechtsgrundlage dies stattfindet und welche Daten verarbeitet werden. Anschließend erfolgt eine kurze Darstellung zu Lob und Kritik der (Fach-)Öffentlichkeit und Behörden. Sodann wird der Einsatz der App im Arbeitsverhältnis näher beleuchtet: Es stellt sich die Frage, ob ein Arbeitgeber die Nutzung der App einseitig anordnen kann, ob Aspekte betrieblicher Mitbestimmung relevant werden und ob der Arbeitgeber das Betreten von Gebäuden und Betriebsstätten von der App abhängig machen kann.

## A. Risikoprognose per App

Seit dem 16.06.2020 steht die Corona-Warn-App in deutschen App-Stores für Android- und iOS-Betriebssysteme kostenlos zum Download bereit. Sie wurde im Auftrag der Bundesregierung von der Deutschen Telekom AG und der SAP SE entwickelt und vom Robert-Koch-Institut (RKI) herausgegeben. Erklärtes Ziel: „Die CWA App soll dazu beizutragen, dass Coronavirus-Infektionsketten schneller erkannt und somit unterbrochen werden können. Um dieses Ziel zu erreichen, soll die CWA App die Nutzer zum einen zuverlässig und schnell über Begegnungen mit anderen infizierten Nutzern informieren und so vor einer möglichen Ansteckung mit dem Coronavirus warnen. Zum anderen sollen die Nutzer in nahezu Echtzeit über ein (positives) Testergebnis informiert werden, so dass sie sich freiwillig isolieren, andere Nutzer warnen und weitere aus epidemiologischer Sicht gebotene Maßnahmen ergreifen können.“[3] Laut Angaben des RKI wurde die App zum 24.07.2020 rund 16,2 Millionen Mal heruntergeladen.[4]

### 1. Wie die App funktioniert[5]

Die App nutzt das Expositionsbenachrichtigungswerkzeug (ENF) für „Privacy-Preserving Contact Tracing“. Das Werkzeug ist Bestandteil der Betriebssysteme Android und iOS.[6] Es ermöglicht Smartphones, wechselnde zufallsgenerierte Kennnummern (sogenannte RPIs) zur Kontaktnachverfolgung auszutauschen. Dafür wird die Funktechnik Bluetooth Low Energy (BLE), eine Technik mit geringem Stromverbrauch, genutzt.[7]

Im ENF wird täglich ein Zufallswert, der sog. Tagesschlüssel (Temporary Exposure Key (TEK)) erzeugt. Aus diesem Tagesschlüssel wird jede 10 bis 20 Minuten ein neuer Entfernungsschlüssel generiert (Rolling Proximity Identifier (RPI)). Der jeweils zuletzt abgeleitete RPI wird vom Smartphone mittels BLE alle fünf Minuten für zwei Sekunden versendet. Gleichzeitig empfängt das Smartphone die auf diese Weise von anderen Smartphones ausgesendeten RPIs. Die empfangenen RPIs nebst Metadaten werden im Kontaktprotokoll des Expositionsbenachrichtigungswerkzeugs für vierzehn Tage gespeichert und anschließend gelöscht. Die Metadaten umfassen das Datum des Kontakts, die Kontaktdauer und die Signalstärke des Bluetooth-Signals.[8]

Wird ein Corona-Test durchgeführt, hat der App-Nutzer die Möglichkeit, einen digitalen Testinformationsprozess zu starten und sich mittels App über das Ergebnis des Tests zu informieren. Er erhält dazu vom Arzt oder Labor einen QR-Code, kann diesen einscannen und sein Testergebnis abfragen. Dies hängt allerdings davon ab, dass das testende Labor an das Serversystem der Corona-Warn-App angeschlossen ist. Der Getestete muss dafür auch im Rahmen der Testdurchführung gesondert in die Übermittlung des Testergebnisses durch das Labor an das Serversystem eingewilligt haben.[9]

Ein nachweislich infizierter Nutzer kann seine Einwilligung erteilen seine Tagesschlüssel zum Abgleich freizugeben und so die Information über das positive Testergebnis verfügbar zu machen.

Die Schlüssel (nun „Positivschlüssel“ genannt) werden auf den Corona-Warn-App-Server geladen und die aktivierten Corona-Warn-Apps aller Nutzer laden regelmäßig die dort hinterlegten Positivschlüssel herunter. Anschließend werden die empfangenen fremden RPIs mit den heruntergeladenen Positivschlüsseln lokal gematcht, um festzustellen, ob ein Nutzer mit einem Infizierten

Kontakt hatte. Passen die Schlüssel zueinander, wird das Übertragungsrisiko bewertet (Risiko-Score) und bei Überschreiten bestimmter Schwellenwerte wird dem App-Nutzer eine Warnung angezeigt.[10] Je nach Art der Begegnung mit einer infizierten Person wird dem Nutzer ein Infektionsrisiko angezeigt. Die App unterscheidet zwischen geringem und erhöhtem Risiko und gibt Handlungsempfehlungen.[11]

Wenn das Labor oder der testende Arzt nicht an die Systeme zur Bereitstellung der Testergebnisse angeschlossen sind, der QR-Code nicht lesbar ist oder kein QR-Code an Labor oder Nutzer ausgegeben wurde, hat ein Nutzer gleichwohl die Möglichkeit sein Ergebnis mittels App zu teilen. Dazu muss der Nutzer eine teleTAN über eine Verifikationshotline erfragen. Dafür muss der Anrufende Plausibilitätsfragen beantworten und wird im nächsten Schritt um Mitteilung seiner Handy-/Telefonnummer gebeten. Durch einen Rückruf wird dem Nutzer eine teleTAN zur Eingabe innerhalb der App zur Verfügung gestellt – diese hat eine Gültigkeit von einer Stunde. Laut Angaben des RKI werde die Nummer spätestens innerhalb einer Stunde gelöscht.[12]

## 2. Datenschutzrechtliche Aspekte

### *a. Verantwortliche Stelle, Rechtsgrundlage und verarbeitete Daten*

Das RKI ist nicht nur Betreiber und Herausgeber der App – es handelt sich bei dem RKI auch um den datenschutzrechtlich Verantwortlichen im Sinne des Art. 4 Nr. 7 DSGVO für die Verarbeitung der personenbezogenen Daten der Nutzer, die mit dem Betrieb der App einhergehen.[13]

Laut Datenschutzerklärung zur App verarbeitet das RKI die anfallenden personenbezogenen Daten im Verhältnis zum App-Nutzer grundsätzlich nur auf Grundlage einer von dem Nutzer erteilten Einwilligung nach Art. 6 Abs. 1 S. 1 lit. a) und Art. 9 Abs. 2 lit. a) DSGVO.[14] Die Rechtsgrundlage stößt auf grundsätzliche datenschutzrechtliche Bedenken: Neben weiteren Voraussetzungen ist ein wesentliches Merkmal für eine wirksame Einwilligung, dass diese freiwillig und damit insbesondere frei von Zwang erteilt wird.[15] Die Freiwilligkeit setzt eine echte Wahlmöglichkeit für die betroffene Person voraus.[16] Insbesondere vor dem Hintergrund eines gewissen sozialen Drucks zur Nutzung der App wird von verschiedenen Seiten diskutiert, ob es an der Freiwilligkeit des Einzelnen fehlen könnte und die Einwilligung als Rechtsgrundlage für die Verarbeitung daher ungeeignet ist.[17] Teile der Literatur geben zu bedenken, dass das Spannungsverhältnis zwischen Freiwilligkeit und effektiver Eindämmung der Infektionen möglicherweise auch nicht hinreichend dadurch aufgelöst werden könne, dass Nutzer nach Installation der App aktiv sowohl der Risikoermittlung als auch dem Teilen des Testergebnisses zustimmen müssen.[18] Vom RKI heißt es dazu: „Das RKI sollte fortwährend beobachten, ob Anzeichen für einen ‚sozialen Zwang' zur Nutzung der CWA-App bestehen und ggf. gegensteuernde Maßnahmen ergreifen."[19]

Gegen eine Freiwilligkeit spricht indes, wenn zwischen dem Verantwortlichen und den Betroffenen ein klares Machtungleichgewicht besteht, etwa dann, wenn es sich bei dem Verantwortlichen um eine Behörde handelt (vgl. ErwG 43 DSGVO). Nach Ansicht des RKI könne aus dem Umstand, dass das RKI als Bundesoberbehörde ein staatliches Organ repräsentiere, allerdings grundsätzlich nicht auf die fehlende Freiwilligkeit geschlossen werden.[20]

Die von der App bzw. dem RKI verarbeiteten Daten können im Wesentlichen in die Kategorien Zugriffs-, Begegnungs- und Gesundheitsdaten unterteilt werden[21]: Zugriffsdaten fallen an, wenn gewisse Funktionen genutzt bzw. aktiviert werden, z.B. die Risikoermittlung, die Testregistrierung oder das Teilen des Testergebnisses. Begegnungsdaten sind die Zufallsnummern, die von dem Smartphone des Nutzers gesendet und empfangen werden können. Dazu zählen auch die Metadaten. Allerdings handelt es sich bei der Kontaktaufzeichnungs-Funktion laut Datenschutzerklärung zur App nicht um einen Bestandteil der App, sondern um einen integralen Bestandteil des Betriebssystems des Smartphones. In der Datenschutzerklärung wird daher ausdrücklich darauf hingewiesen, dass diese Funktion für iPhones von Apple und für Android-Smartphones von Google bereitgestellt werde, die Datenverarbeitung den Datenschutzbestimmungen der genannten Unternehmen unterliege und damit außerhalb des Einflussbereichs des RKI liege.[22] Wird ein Infektionsrisiko ermittelt, sind die Daten als Gesundheitsdaten zu werten.[23] Nach der Legaldefinition aus Art. 4 Nr. 15 DSGVO sind unter Gesundheitsdaten personenbezogene Daten zu verstehen, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen. Gesundheitsdaten liegen auch vor, wenn ein Test registriert wird und wenn der Nutzer ein positives Testergebnis teilt.[24]

Auf der Website des RKI heißt es: „Die App hat keinen Zugriff auf Daten, die einen Nutzer identifizierbar machen. Sichergestellt ist: Eine Corona-positiv getestete Person erfährt nicht, wer informiert wird. Diejenigen, die informiert werden, erfahren nicht, wer die Corona-positive Person ist."[25]

### *b. Lokale Datenverarbeitung – der „dezentrale Ansatz"*

Nach vermehrter Kritik[26] zur ursprünglich präferierten Basissoftware PEPP-PT (Pan-European Privacy-Preserving Proximity Tracing) setzt die Bundesregierung mit der Corona-Warn-App nun auf einen dezentralen Ansatz. Dabei werden die Schlüssel zunächst ausschließlich auf den jeweiligen Smartphones der App-Nutzer gespeichert und nicht auf einem zentralen Server. Erst in dem Fall, dass ein Infizierter sein positives Testergebnis teilen möchte, werden die zufälligen Kontaktkennungen über einen Server an alle Nutzer der Corona-Warn-App übertragen. Das Matchen der Kontakte erfolgt dann lokal auf den Smartphones der anderen App-Nutzer.[27]

## 3. Lob und Kritik der (Fach-) Öffentlichkeit und Behörden

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) Professor Ulrich Kelber positionierte sich zum Start der App wie folgt: „Aus Sicht des Datenschutzes sehe ich keinen Grund, der gegen eine Installa-

tion spricht. [...]". Dennoch gibt er zu bedenken: „Aber es gibt noch Schwachstellen. Dort müssen die verantwortlichen Behörden und Unternehmen Anpassungen vornehmen. Als zuständige Aufsichtsbehörde werden wir überprüfen, dass unsere Hinweise schnellstmöglich umgesetzt werden. [...]". Kritisch sah der BfDI vor allem den Medienbruch von der App zur telefonischen Hotline. So könne der Weg über die Hotline nicht mit einer vollständig pseudonymen Nutzung der App über das automatisierte Verfahren mithalten.[28]

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) äußerte sich mit Pressemitteilung vom 16.06.2020. Sie sehe das „datenschutzfreundliche Grundkonzept als Realisierung des Grundsatzes von Datenschutz by Design." Gleichzeitig stellte sie aber auch klar, dass die Freiwilligkeit nicht durch zweckentfremdende Nutzung untergraben werden dürfe.[29]

Unmittelbar vor der App wurde auch die Datenschutz-Folgenabschätzung (DSFA) veröffentlicht. Bei der DSFA handelt es sich um eine datenschutzrechtliche Risikoanalyse nach Maßgabe des Art. 35 DSGVO. Eine Pflicht zur Durchführung einer DSFA besteht, wenn eine Form der Datenverarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten von Personen hat.[30] Dabei werden die Verarbeitungsvorgänge systematisch identifiziert, bewertet und Abhilfemaßnahmen zur Risikobewältigung geplant. Das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) hat die DSFA zur Corona-Warn-App analysiert: Zunächst lobt das FIfF den Entwicklungsprozess der App, kommt allerdings auch zu dem Ergebnis, dass die DSFA ganz wesentliche grundsätzliche Schwächen aufweise.[31] Hauptmängel der DSFA seien etwa, dass man sich nur auf die App selbst und nicht auf das ganze Verfahren konzentriert habe und, dass man den Verantwortlichen selbst nicht als potentiellen Angreifer einbezogen habe. Zudem sei die Verarbeitung datenschutzrechtlich noch nicht hinreichend durchdrungen worden. Kritisiert wird auch die unzureichende Diskussion effektiver Schutzmaßnahmen zu allen Risiken.[32]

## B. Der Einsatz der Corona-Warn-App im Arbeitsverhältnis

### 1. Kann der Arbeitgeber die Nutzung der App anordnen?

Seit Veröffentlichung der App wird vielfach diskutiert, ob ein Arbeitgeber die Nutzung der App aufgrund seines Direktionsrechts gem. § 106 GewO anordnen kann. Im Hinblick auf die privaten Endgeräte von Arbeitnehmern stößt eine derartige Anordnung allerdings schnell an ihre Grenzen[33], denn die Gestaltung des privaten Lebensbereiches steht außerhalb der Einflusssphäre des Arbeitgebers.[34] In den Bereich der privaten Lebensführung darf durch das Weisungsrecht nach § 106 GewO grds. nicht eingegriffen werden.[35] Eine verpflichtende Nutzungsanordnung durch den Arbeitgeber würde aber gerade in das Privateigentum des Arbeitnehmers eingreifen.[36] Vereinzelte Stimmen in der Literatur ziehen daher in Erwägung, dass eine Anordnung zur Installation der App zumindest auf dienstlich bereitgestellten Smartphones in Betracht kommen könnte.[37] Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) erteilte allerdings kurzerhand eine klare Absage: Ein Arbeitgeber dürfe seine Beschäftigten nicht verpflichten, die Corona-Warn-App auf ihren Smartphones zu nutzen – dies sei datenschutzrechtlich unzulässig. Kein Beschäftigter dürfe verpflichtet werden, durchgängig seine Kontakte und seinen Gesundheitszustand erfassen zu lassen.[38] Dazu führt das BayLDA aus: „Solch massiver Eingriff in die Freiheit des Beschäftigten ist nicht zulässig, da dem Arbeitgeber zum Schutz seiner Beschäftigten mildere Mittel in der Form der allgemeinen Hygienemaßnahmen zur Verfügung stehen. Ein solches Vorgehen würde zudem die vom Anbieter der App, dem Robert-Koch-Institut, in seinen Nutzungsbedingungen festgelegte Freiwilligkeit der Nutzung der App unterlaufen. Diese Rechtslage gilt für private Geräte der Beschäftigten wie für dienstlich bereitgestellte Geräte gleichermaßen."

Das BayLDA sieht hier bereits das Ungleichgewicht im Beschäftigungsverhältnis als Show-Stopper: „Die Einwilligung wäre aufgrund des Ungleichgewichts im Beschäftigungsverhältnis in aller Regel als nicht freiwillig und damit datenschutzrechtlich unwirksam anzusehen."[39]

Zudem ergibt sich ein beschränkter Nutzen der Risikowertermittlung durch die App, wenn der Beschäftigte das Smartphone nicht ständig bei sich führt.[40] Wenn das Endgerät etwa nur während der Arbeitszeit am Körper getragen wird, beschränkt sich die Risikobetrachtung eben auch nur auf diese Zeiträume. Eine Erfassung wäre aber überhaupt nur dann sinnvoll, wenn sich diese auch auf die Freizeit erstrecken würde.[41]

Ob die bloße Empfehlung eines Arbeitgebers, die App zu nutzen, ein gangbarer Weg ist, wirft gleichermaßen Fragen im Hinblick auf einen gewissen sozialen Druck auf[42] und bedarf einer gesonderten Betrachtung.

### 2. Corona-Warn-App als Fall betrieblicher Mitbestimmung?

Im Zusammenhang mit der Corona-Warn-App im Arbeitsverhältnis stellt sich auch die Frage nach Aspekten betrieblicher Mitbestimmung[43]: So hat der Betriebsrat beispielsweise gem. § 87 Abs. 1 Nr. 1 BetrVG, soweit eine gesetzliche oder tarifliche Regelung nicht besteht, ein Mitbestimmungsrecht bei Fragen der Ordnung des Betriebs und des Verhaltens der Arbeitnehmer im Betrieb. Zudem besteht gem. § 87 Abs. 1 Nr. 7 BetrVG ein Mitbestimmungsrecht bei Regelungen über den Gesundheitsschutz im Rahmen der gesetzlichen Vorschriften. Relevant wäre auch eine Mitbestimmung aus § 87 Abs. 1 Nr. 6 BetrVG, wenn man Einführung und Anwendung der App als eine technische Einrichtung zu werten hätte, die dazu bestimmt ist, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen.[44]

Allerdings wird auch die betriebliche Mitbestimmung nicht darüber hinweghelfen können, dass sich die Weisungsbefugnis eines Arbeitgebers (als Betriebspartei) nicht auf die privaten Lebensbereiche des Arbeitnehmers erstreckt.[45] Abgesehen davon wird aber auch im Hinblick auf die dienstlichen Smartphones der Grundsatz der Freiwilligkeit der Corona-Warn-App einer Nutzungsanordnung entgegenstehen.[46] Bei




Bild: iStock

einer Betriebsvereinbarung wird es sich insoweit nicht um einen geeigneten datenschutzrechtlichen Erlaubnistatbestand handeln.[47]

### 3. Kann der Zugang zu Gebäuden/Arbeitsstätten vom Vorweisen der App abhängig gemacht werden?

Zudem stellt sich die Frage, ob der Zugang zu Gebäuden und Arbeitsstätten vom Vorweisen der App abhängig gemacht werden kann. In diesem Zuge wird diskutiert, ob Einzelnen der Zutritt etwa auf Grundlage des Hausrechts verweigert werden kann.

Die DSK hat mit Pressemitteilung vom 16.06.2020 allerdings ausdrücklich klargestellt, dass der Zugang zu Gebäuden/Arbeitsstätten nicht vom Vorweisen der Corona-Warn-App abhängig gemacht werden dürfe. Bei einem solchen Vorhaben handle es sich um eine zweckwidrige Verwendung der App, die bereits mit dem Konzept der Freiwilligkeit nicht vereinbar sei. Zudem sei eine Diskriminierung von Personen, die die App nicht anwenden, auszuschließen.[48]

Schon unmittelbar zum Start der App mahnte der BfDI: „Es ist in keinem Fall zulässig, dass Dritte Einblick in die App fordern. Ich kann die Inhaber von Geschäften oder öffentlichen Verkehrsmitteln nur dringend warnen: Versucht es erst gar nicht!“[49]

### 4. Pflicht zur Mitteilung eines erhöhten Infektionsrisikos

Überdies stellt sich die Frage, ob ein Arbeitnehmer, der die Corona-Warn-App nutzt, seinem Arbeitgeber mitzuteilen hat, wenn die App ihn im Hinblick auf ein erhöhtes Infektionsrisiko warnt. Zunächst ist zu beachten, dass sowohl Arbeitgeber als auch Arbeitnehmer im Arbeitsverhältnis gewissen Schutz- und Rücksichtnahmepflichten als Nebenpflichten aus ihrem Arbeitsvertrag unterliegen. Zudem unterliegt ein Arbeitgeber auch Schutzmaßnahmen gegenüber weiteren Beschäftigten, etwa nach § 3 Abs. 1 ArbSchG, § 618 BGB. Vor diesem Hintergrund halten es Stimmen in der Literatur in bestimmten Konstellationen durchaus für möglich, dass dem Arbeitgeber der Umstand eines erhöhten Infektionsrisikos aus der App verpflichtend anzuzeigen sei, selbst, wenn dies mit Blick auf die Freiwilligkeit der App zunächst widersprüchlich erscheinen möge.[50] In derartigen Fällen sei eine Interessenabwägung im Einzelfall vorzunehmen, die zum einen den Schutz des Betroffenen vor Preisgabe der eigenen besonders geschützten Gesundheitsdaten und zum anderen erhebliche Gesundheits- und Ansteckungsgefahren für Dritte berücksichtige.[51]

## C. Fazit

Die Corona-Warn-App fußt auf dem Grundsatz der Freiwilligkeit. Deutsche Aufsichtsbehörden erteilen einer einseitigen Anordnung zur Nutzung eine Absage. Insbesondere kann der Zugang zu Gebäuden/Arbeitsstätten nicht vom Vorweisen der App abhängig gemacht werden. Unter Umständen könnte sich eine Pflicht zur Information des Arbeitgebers bei der Warnung vor einem erhöhten Infektionsrisiko ergeben.

Redaktionsschluss 26.07.2020.

1 Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

2 Im Einzelnen dazu: Bundesfinanzministerium, 22.05.2020, „Kampf gegen Corona: Größtes Hilfspaket in der Geschichte Deutschlands“, abrufbar unter: https://www.bundesfinanzministerium.de/Content/DE/Standardartikel/Themen/Schlaglichter/Corona-Schutzschild/2020-03-13-Milliarden-Schutzschild-fuer-Deutschland.html, abgerufen am 26.07.2020.

3 Robert-Koch-Institut, Bericht zur Datenschutz-Folgenabschätzung für die Corona-Warn-App der Bundesrepublik Deutschland, Version 1.0.1, 18.06.2020, abrufbar unter: https://www.coronawarn.app/assets/documents/cwa-dateschutz-folgenabschaetzung.pdf, abgerufen am: 26.07.2020, (künftig zitiert mit RKI, Bericht zur DSFA, En. 3), S. 43.

4 Stichtag 24.06.2020; Aktuelle Downloadzahlen stellt das RKI zur Verfügung unter: RKI, „Infektionsketten digital unterbrechen mit der Corona-Warn-App“, abrufbar unter: https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/WarnApp/Warn_App.html, abgerufen am 25.07.2020.

5 Dies ist eine vereinfachte Darstellung - zur Funktionsweise der App im Detail: RKI, Bericht zur DSFA, En. 3.

6 Android ab Version 6 und iOS ab Version 13.5.

7 RKI, Bericht zur DSFA, En. 3, S. 43.

8 RKI, Bericht zur DSFA, En. 3, S. 60 f.

9 Robert-Koch-Institut, Datenschutzerklärung Corona-Warn-App, abrufbar unter: https://www.coronawarn.app/assets/documents/cwa-privacy-notice-de.pdf; abgerufen am: 26.07.2020 (künftig

zitiert mit RKI, Datenschutzerklärung Corona-Warn-App, En. 9).

10 Vgl. Robert-Koch-Institut, „Infektionsketten digital unterbrechen mit der Corona-Warn-App“, Stand 24.07.2020, abrufbar unter: https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/WarnApp/Warn_App.html, abgerufen am 25.07.2020 (künftig zitiert mit RKI, Infektionsketten unterbrechen, En. 10), „Wie die Risikofaktoren errechnet werden“ (Stand 14.07.2020).

11 RKI, Infektionsketten unterbrechen, En. 10, Wie die Corona-Warn-App über ein mögliches Infektionsrisiko informiert (Stand 16.06.2020).

12 Dazu im Einzelnen RKI, Bericht zur DSFA, En. 3, S. 53 f.; RKI, Datenschutzerklärung Corona-Warn-App, En. 9.

13 RKI, Bericht zur DSFA, En. 3, S. 43; RKI, Datenschutzerklärung Corona-Warn-App, En. 9.

14 RKI, Datenschutzerklärung Corona-Warn-App, En. 9.

15 Heckmann/Paschke, in: Ehmann/Selmayr, DSGVO Kommentar, 2. Aufl. 2018, Art. 7 DSGVO, Rn. 48, künftig zitiert mit Heckmann/Paschke, DSGVO.

16 Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF), Datenschutz-Folgenabschätzung für die Corona App, Version 1.6 – 29. April 2020, abrufbar unter: https://www.fiff.de/dsfa-corona-file/at_download/file, abgerufen am 26.07.2020), künftig zitiert mit FIfF, DSFA für die Corona App, En. 16, S. 54 mit Verweis auf Article 29 Data Protection Working Party 2018, S. 5; Heckmann/Paschke, DSGVO, Art. 7 DSGVO, Rn. 50.

17 Zur Diskussion m.w.N.: RKI, Bericht zur DSFA, En. 3, S. 88 f.

18 Köllmann, NZA 2020, 831 (832) mit Verweis auf FIfF, DSFA für die Corona App, En. 16, S. 55.

19 RKI, Bericht zur DSFA, En. 3, S. 90.

20 RKI, Bericht zur DSFA, En. 3, S. 88; a.A. FIfF, DSFA für die Corona App, En. 16, S. 54.

21 Einzelheiten nachzulesen in RKI, Datenschutzerklärung Corona-Warn-App, En. 9.

22 RKI, Datenschutzerklärung Corona-Warn-App, En. 9.

23 So auch die Struktur des RKI, Datenschutzerklärung Corona-Warn-App, En. 9.

24 Dazu im Einzelnen RKI, Bericht zur DSFA, En. 3, S. 82 f.

25 RKI, Infektionsketten unterbrechen, En. 10, Warum die Daten der Nutzerinnen und Nutzer sicher und geschützt sind (Stand: 16.06.2020); kritisch zum Personenbezug im Rahmen der Corona-Warn-App Pentzien/Lösch, DSB 2020, 178 (179 f.).

26 Chaos Computer Club, 24.04.2020, Corona-Tracing-App: Offener Brief an Bundeskanzleramt und Gesundheitsminister, abrufbar unter: https://www.ccc.de/de/updates/2020/corona-tracing-app-offener-brief-an-bundeskanzleramt-und-gesundheitsminister, abgerufen am: 26.07.2020.

27 Bayerisches Landesamt für Datenschutzaufsicht, Corona-Warn-App, abrufbar unter: https://www.lda.bayern.de/de/thema_corona_warn_app.html, abgerufen am 26.07.2020 (künftig zitiert mit LDA Bayern, CWA, En. 27); RKI, Infektionsketten unterbrechen, En. 10, Warum die Daten der Nutzerinnen und Nutzer sicher und geschützt sind (Stand 16.06.2020).

28 Der Bundesbeauftragte für den Datenschutz und die Informationssicherheit (BfDI), Pressemitteilung v. 16.06.2020, „Datenschutz bei Corona-Warn-App ausreichend“, abrufbar unter: https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2020/12_Corona-Warn-App.html, abgerufen am 26.07.2020, künftig zitiert mit BfDI, Pressemitteilung 16.06.2020, En. 28.

29 DSK, Pressemitteilung v. 16.06.2020, „Datenschutzfreundliches Grundkonzept der Corona-Warn-App – Freiwilligkeit darf nicht durch zweckwidrige Nutzung untergraben werden!“, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/pm/20200616_pm_corona_warn_app.pdf, abgerufen am 26.07.2020, künftig zitiert mit DSK, Pressemitteilung 16.06.2020, En. 29.

30 Vgl. Art. 35 Abs. 1 DSGVO.

31 FIfF, Analyse und konstruktive Kritik der offiziellen Datenschutz-Folgenabschätzung der Corona-Warn-App, Version 1.0.-29.06.2020, S. 1, abrufbar unter: https://www.fiff.de/dsfa-corona-kritik/at_download/file, abgerufen am 26.07.2020 (künftig zitiert mit FIfF, Analyse und konstruktive Kritik, En. 31.

32 FIfF, Analyse und konstruktive Kritik, En. 31, S. 1.

33 Köllmann, NZA 2020, 831 (835); Fuhlrott, GWR 2020, 275 (276).

34 Vgl. BAG, Urt. v. 23.06.1994 - 2 AZR 617/93, NZA 1994, 1080 (1082).

35 BAG, Urt. v. 23.08.2012 – 8 AZR 804/11, NZA 2013, 268 (270).

36 Dazu im Einzelnen Köllmann, NZA 2020, 831 (835).

37 So etwa Giese, „Die Corona-App: Ein Muss oder Kann im Arbeitsverhältnis?“, 17.06.2020, abrufbar unter https://www.arbeitsrecht-weltweit.de/2020/06/17/die-corona-app-ein-muss-oder-kann-im-arbeitsverhaeltnis, abgerufen am: 26.07.2020; a.A. im Ergebnis auch Köllmann, NZA 2020, 831 (835); Fuhlrott, GWR 2020, 275 (276).

38 LDA Bayern, CWA, En. 27; ebenso der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz, „Kugelmann pocht auf Freiwilligkeit der Corona-Warn-App – Sie darf nicht zur Eintrittskarte werden“, 25.06.2020, abrufbar unter: https://www.datenschutz.rlp.de/de/aktuelles/detail/news/detail/News/kugelmann-pocht-auf-freiwilligkeit-der-corona-warn-app-sie-darf-nicht-zur-eintrittskarte-werden/, abgerufen am 26.07.2020.

39 LDA Bayern, CWA, En. 27.

40 Köllmann, NZA 2020, 831 (835).

41 LDA Bayern, CWA, En. 27.

42 Köllmann, NZA 2020, 831 (835), Fn. 66.

43 Zur Mitbestimmung im Zusammenhang mit der Corona-Warn-App im Einzelnen Köllmann, NZA 2020, 831 (835 f.); Fuhlrott, GWR 2020, 275 (277).

44 Mangels Leistungs- und Verhaltenskontrolle ablehnend Köllmann, NZA 2020, 831 (836), es sei denn ein Arbeitgeber könne die tatsächliche Installation und Verwendung auf dem dienstlichen Smartphone kontrollieren.

45 Köllmann, NZA 2020, 831 (836) mit Verweis auf BAG, Beschl. v. 22.07.2008 –1 ABR 40/07, NZA 2008, 1248.

46 Köllmann, NZA 2020, 831 (836).

47 Vgl. Fuhlrott, GWR 2020, 275 (276); Köllmann, NZA 2020, 831 (836);

48 DSK, Pressemitteilung 16.06.2020, En. 29.

49 BfDI, Pressemitteilung 16.06.2020, En. 28.

50 So Fuhlrott, GWR 2020, 275 (276).

51 Fuhlrott, GWR 2020, 275 (276); für eine Interessenabwägung im Einzelfall auch Köllmann, NZA 2020, 831 (834).

Dr. Susanne Holzgraefe

# Die Tücken der Heimarbeit

Die Regierung spricht von *Heimarbeit*, der Volksmund von *HomeOffice*. Es entsteht der Eindruck, als hätte sich das Verständnis der beiden Begriffe in Corona-Zeiten etwas verschoben. Allerdings führten die Begriffe auch schon vor Corona zu unterschiedlichen Ansichten ihrer Bedeutung. In dem Zusammenhang, dass Beschäftigte zur Erbringung ihrer Leistung örtlich ausgelagert werden, fallen daneben auch häufiger die Begriffe: *Mobiler Arbeitsplatz* und *Work-from-Anywhere*. Auch hier gibt es verschiedene Ideen, was sich genau hinter den Begriffen verbirgt. Die Pandemie hat gezeigt, dass Beschäftigte nicht nur in Heimarbeit geschickt wurden, sondern auch häufig vor der *Bring Your Own Device* (BYOD) Problematik stehen.

Um das Thema Datenschutz unter dem Aspekt, dass Arbeitsplätze örtlich ausgelagert sind, genauer unter die Lupe nehmen zu können und Missverständnisse zu vermeiden, ist es erforderlich, die Begriffe, wie sie hier im Artikel verwendet werden, einmal zu definieren und jede der vier genannten Situationen einzeln zu betrachten.

Um die Gesetze und Vorschriften zum Datenschutz auch bei den unterschiedlich vorliegenden Bedingungen der Arbeitsplätze zu gewährleisten, sollten im Vorfeld die Maßnahmen, nicht nur die technischen sondern vor allem auch die organisatorischen, genau durchdacht werden.

### Geltung von Gesetzen und Vorschriften

Die Gesetze und Vorschriften zum Datenschutz gelten natürlich völlig unabhängig von der genaueren Spezifikation der Arbeitsbedingungen. Die Verantwortlichen bleiben verantwortlich, egal ob Angestellte zu Hause am Küchentisch oder auf hoher See in der Kajüte eines Segelschiffes ihre Tätigkeit ausführen. Der genaue Dienstort spielt dennoch eine entscheidende Rolle.

Nicht nur Feiertage, Mindest- und Bildungsurlaub sowie das zuständige Arbeitsgericht sind von dem Dienstort abhängig, sondern ggf. auch die Gesetze und Vorschriften zum Datenschutz. Ändert sich der Ort der Datenverarbeitung, ist zu prüfen, ob weitere lokale Gesetze und Vorschriften einzuhalten sind. Hat zum Beispiel ein schwedisches Unternehmen Beschäftigte im HomeOffice in Deutschland mit der Verarbeitung personenbezogener Daten betraut, sollte das Unternehmen nicht nur die DSGVO sowie ggf. schwedische Gesetze im Blick haben, sondern auch das BDSG.

Wohnen in Deutschland angestellte zum Beispiel in Belgien, den Niederlanden oder Österreich, so ist zu bedenken, dass bei einer Auslagerung des Dienstortes an die Wohnorte der Beschäftigten sich plötzlich nicht nur die Feiertage und arbeitsrechtlichen Bedingungen für die entsprechenden Personen ändern, sondern je nach Aufgabenbereich ggf. auch andere Datenschutzvorschriften einzuhalten sind. Spannend wird es hier, wenn Nicht-EU-Länder, wie die Schweiz, beteiligt sind.

Öffentliche Stellen, die ihre Beschäftigten in die Heimarbeit schicken, sollten dabei darüber hinaus bedenken, dass Beschäftigte durchaus in anderen Bundesländern wohnen können. Findet zum Beispiel die Datenverarbeitung eines Jugendamtes in NRW plötzlich in Niedersachsen statt, ist zu prüfen, inwieweit jetzt zusätzlich das niedersächsische Landesdatenschutzgesetz Anwendung findet.

### Corona Fauxpas

Plötzlich Lockdown, plötzlich Abstand halten. Plötzlich rät die Regierung zur Heimarbeit und viele öffentliche Stellen sowie Unternehmen der freien Wirtschaft reagieren postwendend.

*„Wir leiten jetzt alle E-Mails, selbst die mit sensiblen Informationen zu einzelnen Kindern, unverschlüsselt an die privaten E-Mail-Adressen der Beschäftigten weiter, die ab sofort zu Hause arbeiten, weil wir es technisch nicht umgesetzt haben, dass die Beschäftigten E-Mails auch ausserhalb des im Verwaltungsbüro stehenden Computers empfangen können, und wir darüber hinaus für die Weiterleitung noch keine Verschlüsselungsmethoden eingerichtet bzw. eingeführt haben."*

Das ist nur eine der vielen Aussagen sowohl aus öffentlichen Verwaltungen als auch der freien Wirtschaft während des Corona-Lockdowns, die Datenschützern den Atem stocken ließ. Noch mehr, wenn Verantwortliche und auch Personen in der Politik das dann auch noch mit *„Kavaliersdelikt"* oder *„das müsse man doch verstehen, dass das nunmal jetzt während der Pandemie nicht anders ginge"* lässig abwedelten.

Dass private E-Mail-Adressen durchaus häufiger von der ganzen Familie genutzt werden, und so Partner, Kinder, Eltern oder auch Freunde - häufig die Freunde, die sich mit Computern besser auskennen - die Zugangsdaten zu den privaten E-Mail-Konten haben, kommt hier aus Sicht von Sicherheit und Datenschutz noch erschwerend hinzu.

Gerne werden die Personen, die auf die Problematik aufmerksam machen, als *„Verschwörungstheoretiker"* abgestempelt und abhängig Beschäftigte laufen dabei Gefahr, als Störenfried des Betriebsklimas angesehen zu werden und auf der Abschussliste zu landen.

Wie gravierend die Folgen der Datenpannen, die während der Corona-Pandemie entstanden sind, sowie Sensibilisierungsdefizite von Beschäftigten sind, lässt sich nur schwer erahnen. Es zeigt sich jedoch, wie wichtig es ist die Auslagerung von Beschäftigten genau zu planen, Maßnahmen zu überdenken und technische Sicherheitsanforderungen im Vorfeld umzusetzen.

### Homeoffice

Wörtlich übersetzen lässt sich das Wort HomeOffice mit *heimisches Büro*. Einer der Pioniere im Bereich HomeOffice war der schwedische Softwarehersteller MySQL AB (heute Oracle). Sie wollten für ihre Software die weltweit besten Programmiererinnen und Programmie-

rer unter Vertrag nehmen, ohne dass sie samt Familien nach Uppsala umsiedeln mussten. Das Unternehmen entwickelte Voraussetzungen und Strategien, so dass alle Beschäftigten ihren Dienstort in der Nähe ihres Wohnortes hatten. Die Autorin hatte das Glück mehrere Jahre Teil dieses Unternehmens zu sein. Die Zufriedenheit der Beschäftigten hatte oberste Priorität. Die vielen unterschiedlichen, dienstortabhängigen Vorschriften zu beachten war nicht immer einfach.

HomeOffice muss natürlich nicht immer gleich länderübergreifend sein. Auch gibt es Unternehmen, bei denen sich zukünftig Beschäftigte zwischen überwiegend Homeoffice oder überwiegend am Sitz des Unternehmens entscheiden können. Dem *Teil-HomeOffice* ist der nachfolgende Abschnitt gewidmet.

HomeOffice, wie es hier im Artikel verwendet wird, ist das selbstverwaltete Büro am Wohnort. Der Dienstort ist in der Nähe des Wohnortes. Hierbei ist egal, ob sich das Büro im Haus bzw. der Wohnung des Beschäftigten befindet, sich Beschäftigte jeweils einen Büroraum anmieten oder sich in ein Gemeinschaftsbüro einmieten. Sind mehrere Beschäftigte an einem Ort ansässig, können sie auch gemeinsam Bürofläche für ihre Arbeitsplätze anmieten.

Der Dienstort wird im Arbeitsvertrag festgelegt. Es gelten die dienstortabhängigen, rechtlichen Bestimmungen für diesen Dienstort. Verantwortlich bleibt aber nach wie vor die Arbeitgeberin. Daher ist es ratsam, die Gestaltung des Dienstortes nicht nur unter Berücksichtigung ergonomischer Aspekte, sondern vor allem auch unter Einhaltung der Datenschutz-, Sicherheits- und IT-Sicherheits-Aspekte vertraglich zu regeln.

Damit Beschäftigte später nicht mit Art. 13 GG (Schutz der eigenen Wohnung) winken, wenn Vertretende der Arbeitgeberin wie zum Beispiel die IT-Sicherheits- oder die Datenschutzbeauftragte vorbeikommen, um sich von der Einhaltung der Vorschriften vor Ort zu überzeugen, ist es ratsam, auch das im Vertrag festzuschreiben. Darüber hinaus bedarf es ggf. vertraglicher Regelungen zu Kunden- und Kollegenbesuchen sowie der Bereitstellung eines Arbeitsplatzes im HomeOffice für Auszubildende. Auch ratsam ist, Betriebsprüfungen und Durchsuchungen bei den Verhandlungen zu bedenken.

Die Definition des hier dargestellten HomeOffice ist quasi eine Mikroniederlassung des Unternehmens, die von den jeweiligen Angestellten selbst verwaltet wird. Hierbei stellt sich dann auch die Frage, wer das Büro sauber hält und wie das mit dem Zugang der Familie aussieht.

Wird ein Anstellungsverhältnis im HomeOffice von Anfang an angestrebt, lässt sich alles im Anstellungsvertrag regeln. Schwierig wird es jedoch, wenn in einem bestehenden Anstellungsverhältnis auf HomeOffice umgestellt werden soll. Immerhin ist es eine Dienstort-Änderung und die Voraussetzungen für das jeweilige Büro am Wohnort der Beschäftigten müssen auch erstmal geschaffen werden.

### Teil-Homeoffice

Teil-HomeOffice, auch *partielles HomeOffice* genannt, sieht vor, dass Beschäftigte zum einem ihr, wie oben schon beschrieben, selbst verwaltetes Büro am Wohnort haben und das Unternehmen ihnen daneben noch einen festen Arbeitsplatz im Sitz des Unternehmens zur Verfügung stellt, so dass die Beschäftigten zum Beispiel dienstags und mittwochs Homeoffice machen, montags, donnerstags und freitags in ihrem Büro im Unternehmen anzutreffen sind. Für viele ortsabhängige rechtliche Grundlagen ist hier ausschlaggebend, wo sich Beschäftigte häufiger aufhalten. Zum Beispiel für Feiertage, Bildungsurlaub und je nach Tätigkeit auch für die Gesetze und Vorschriften zum Datenschutz.

Für die Gesetze und Vorschriften des Datenschutzes ist zu bedenken, dass, auch wenn die Datenverarbeitung nur zu einem geringen Prozentsatz in einem anderen Bundesland ausgeführt wird, zu prüfen ist inwieweit hier die Datenschutzbestimmungen des entsprechenden Landes bzw. Bundeslandes zu beachten sind.

### Heimarbeit

Heimarbeit wird in diesem Artikel als etwas völlig anderes definiert als das HomeOffice. Früher wurden Krabben in Heimarbeit an norddeutschen Küchentischen gepult oder Kugelschreiber am heimischen Wohnzimmertisch zusammengebaut. Heimarbeit war etwas für Tätigkeiten, die keinen Geschäftsgeheimnissen unterlagen. Doch das hat sich geändert.

Heute werden auch Tätigkeiten am heimischen Küchen- oder Wohnzimmertisch verrichtet, die nicht nur Geschäftsgeheimnisse beinhalten, sondern durchaus auch datenschutz- und IT-sicherheitskritisch sind.

Eine von vielen Schwierigkeiten dabei ist, dass sich Art. 13 GG (Schutz der eigenen Wohnung) hier nicht so einfach durch vertragliche Regelung umgehen lässt wie beim HomeOffice, da ja quasi die gesamte Wohnung zum Arbeitsplatz wird und nicht nur ein einzelner Raum für die abhängigen Tätigkeiten zur Verfügung gestellt wird. Eine Überprüfung durch die Verantwortlichen, ob die Datenverarbeitung vor Ort ordnungsgemäß abläuft, kann schwierig werden.

Eine Trennung zwischen privat und geschäftlich ist für Beschäftigte weit schwieriger als beim HomeOffice. Da sie hier nicht einfach nur eine Tür schließen können, ist die Gefahr groß, dass die Arbeit Teil des Privatlebens wird. Anwesende Familienmitglieder und Besucher können ungewollt automatisch Ohren- und ggf. sogar Augenzeugen von Audio- und Video-Chats sowie Telefongesprächen werden.

Bei der Heimarbeit wird die Wohnung des Beschäftigten zum Dienstort und es gelten die an dem Ort geltenden, dienstortabhängigen, rechtlichen Bestimmungen. Genau wie beim HomeOffice sollte selbst bei nur teilweise in Heimarbeit verarbeiteten personenbezogenen Daten geprüft werden, inwieweit hier die Datenschutzbestimmungen des entsprechenden Landes bzw. Bundeslandes, in dem sich die Wohnung befindet, zu beachten sind.

Schwierig ist natürlich auch hier, Beschäftigte von jetzt auf gleich in Heimarbeit zu schicken. Von der Fraglichkeit der Freiwilligkeit abgesehen handelt es sich auch hier um einen Dienstortwechsel und Beschäftigte müssen dafür zu Hause ggf. vorher noch die eine oder andere Vorkehrung bzw. Voraussetzung schaffen, dass ein Arbeiten von zu Hause überhaupt möglich ist.

Es ist ratsam im Vorfeld genau zu prüfen, wie hoch das Risiko ist, wenn

personenbezogene Daten in Heimarbeit verarbeiten werden.

**Mobiler Arbeitsplatz**

Mobiler Arbeitsplatz bedeutet hier in diesem Artikel, dass die Arbeitsmittel, wie Computer, nicht fest installiert sind, sondern mobile Geräte, wie Laptops, Tablets und Smartphones genutzt werden. Dadurch sind Beschäftigte flexibel und können sowohl in einer Niederlassung der Arbeitgeberin, als auch im HomeOffice oder in Heimarbeit arbeiten.

Mobiler Arbeitsplatz bedeutet hier noch nicht, dass Beschäftigte von überall arbeiten sollten, sondern nur, dass die verwendeten Geräte an verschiedenen Orten innerhalb des Unternehmens sowie beim Kunden oder im HomeOffice genutzt werden können. Auch das Arbeiten während Dienstreisen, zum Beispiel in der Bahn oder im Flieger, wird damit möglich.

Mobile Arbeitsplätze sind sehr beliebt und es ist ratsam, hier sehr gut durchdachte technische und organisatorische Maßnahmen zu entwickeln, die das datenschutzfreundliche Arbeiten in allen Filialen, beim Kunden, in der Bahn usw. abdecken.

**Work-from-Anywhere**

Egal ob am Nordseestrand, auf Mallorca oder daheim am Esstisch: *Work-from-Anywhere* soll dem Beschäftigten die Möglichkeit bieten von überall zu arbeiten. Einen festen Dienstort soll es dabei eigentlich nicht geben. Das Modell hakt alleine schon durch die Tatsache, dass es eine Reihe dienstortabhängiger rechtlicher Bestimmungen gibt.

Die Überwachung der Verarbeitung von personenbezogenen Informationen durch die Verantwortlichen bzw. die betrieblichen Datenschutzbeauftragten könnte schwierig werden, wenn der Beschäftigte plötzlich am anderen Ende der Welt ist.

Es ist hier ratsam im Vorfeld genau zu prüfen, wie hoch das Risiko ist, wenn personenbezogene Daten von Beschäftigten verarbeitet werden, die *Work-from-Anwhere* vertraglich vereinbart haben.

**Bring Your Own Device (BYOD)**

Köche mögen ihre eigenen Messer mitbringen, Friseure ihre eigenen Scheren. Weder die Messer noch die Scheren speichern Informationen zu anderen Personen. Vielleicht ist in das Messer bzw. die Schere ein Name eingraviert und anhand der Abnutzung können findige Augen erkennen, wem das Werkzeug gehört. An der Friseurschere mögen vielleicht auch noch DNA-Spuren des letzten Kunden zu finden sein. Das Datenschutzrisiko ist hier aber dennoch extrem gering. Ob die Köchin ihr Messer oder die Friseurin ihre Schere auch noch privat nutzt, macht hier aus Sicht des Datenschutzes keinen Unterschied.

Bei Computern, Laptops, Tablets oder Smartphones sieht das Ganze anders aus. Nutzen Beschäftigte ihre eigenen Geräte sowohl privat als auch für die Arbeit, so ist die Gefahr groß, dass sich private und geschäftliche Informationen mischen.

*„Unsere Kinder konnten die Schulaufgaben nicht erledigen, weil wir den einzigen Computer, den wir besitzen, für unsere Tätigkeit im Homeoffice brauchten."*

Eine von vielen Entschuldigungen, warum einige Kinder während des Lockdowns die gestellten Aufgaben nicht erledigten. Ob es sich hierbei um eine Ausrede oder die Wahrheit handelt, spielt keine Rolle. Es zeigt, dass es durchaus üblich ist, dass Kinder keine eigenen Computer haben. Es zeigt auch, dass es in Familien durchaus nur einen Computer gibt, der von allen Familienmitgliedern genutzt wird. Auch das Smartphone der Eltern durfte in vielen Familien während des Lockdowns für die Schulaufgaben genutzt werden. Ob hier wirklich alle von der Arbeitgeberin vorgegebenen, für die Einhaltung des Datenschutzes erforderlichen, technischen und organisatorischen Maßnahmen umgesetzt wurden, bleibt fraglich.

Wie sieht das mit der Datenschutz-Risikobewertung aus, wenn die ganze Familie Zugriff auf die Geräte hat, mit Hilfe derer der geschäftlichen Tätigkeit nachgegangen wird?

BYOD birgt bei IT-Geräten und Smartphones immer die Schwierigkeit der gemischten Privat- und Geschäftsnutzung. Bei Smartphones kennt dadurch darüber hinaus die Arbeitgeberin die private Telefonnummer. Die Gefahr, dass die Arbeitgeberin das ausnutzt und außerhalb der Arbeitszeiten oder während des Erholungsurlaubs anruft, besteht. Erfahren Kunden die Nummer, besteht auch die Gefahr, dass diese außerhalb der Arbeitszeiten anrufen.

Die Prüfung, inwieweit BYOD in Deutschland überhaupt in Ordnung ist, bleibt den Juristen überlassen. Sollten nicht eigentlich die für die Ausführung der Tätigkeit notwendigen Arbeitsmittel von der jeweiligen Arbeitgeberin zur Verfügung gestellt oder die Kosten dafür übernommen werden?

**Fazit**

Die Corona-Pandemie hat gezeigt, dass eine plötzliche Auslagerung der Beschäftigten in Heimarbeit, ohne die notwendigen technischen und organisatorischen Maßnahmen dafür genau zu durchdenken und Datenschutz-Risiken unbeachtet zu lassen, keine gute Idee ist. Darüber hinaus auch noch auf die Schnelle BYOD einzuführen führt ins Chaos.

Sollen die Beschäftigten im selbstverwalteten HomeOffice in der Nähe ihres Wohnortes arbeiten statt in einem festen Büro in einer Firma, so ist es ratsam, hier vertraglich Regelungen zur Kontrolle durch Vertretende des Unternehmens sowie dessen Datenschutzbeauftragten zu finden, genauso wie den Besuch von Betriebsprüfern, Kunden, Auszubildenden und Kollegen vertraglich zu regeln.

Der Dienstort ist entscheidend für viele rechtliche Bestimmungen. Inwieweit hier auch die Datenschutz-Gesetze und -Vorschriften, die am Dienstort gelten, zu berücksichtigen sind ist im Einzelfall zu prüfen.

Personenbezogene Datenverarbeitung in Heimarbeit oder gar in einem Work-from-Anywhere-Konzept ausführen zu lassen sollte wohl durchdacht sein.

Die Nutzung privater Geräte für dienstliche Tätigkeiten ist auch in Coronazeiten mit äußerster Vorsicht genauestens zu überlegen.

Egal wo außerhalb des Unternehmens und mit welchen Geräten gearbeitet wird, die Ausarbeitung und Umsetzung von technischen und orgnisatorischen Maßnahmen, die einen Datenabfluß eindämmen, sind unumgänglich. Mögliche Datenschutz-Pannen und deren Risiken sollten von allen Seiten durchleuchtet werden.

Julia Reda

# PimEyes & Gesichtserkennung in Europa

**Edit Policy: – wo bleibt der Aufschrei?**

Gesichtserkennung ist eine massive Gefahr für die Grundrechte, aber eine Debatte über ihren Einsatz gibt es in Deutschland und Europa nicht. Anders in den USA.

Gesichtserkennung stellt eine erhebliche Gefahr für unsere Grundrechte dar. Hierzulande muten Debatten über das Thema oft so an, als handele es sich dabei um Zukunftsmusik – oder ein Problem, das in erster Linie Länder mit einem niedrigeren Datenschutzniveau wie die USA oder China betreffe. Dabei breitet sich die automatische Gesichtserkennung in Europa und auch in Deutschland rasant aus. Bundespolizei und Kriminalämter setzen die Technologie bereits seit Jahren ein, Tendenz stark steigend. Die EU-Kommission investiert in unseriöse Startups, die Gesichtserkennung an Europas Außengrenzen als Lügendetektoren einsetzen wollen. Und ein polnisches Clearview-Klon bietet eine frei zugängliche Gesichter-Suchmaschine im Netz an. Wo bleibt der Aufschrei?

## Das Geschäft mit biometrischer Massenüberwachung

In einer *umfangreichen Recherche* hat Netzpolitik kürzlich auf PimEyes aufmerksam gemacht, ein polnisches Gesichtserkennungs-Startup, das die anonyme Suche nach beliebigen Gesichtern in einer Datenbank aus 900 Millionen, augenscheinlich aus öffentlichen Quellen stammenden, Bildern erlaubt. Auch Screenshots aus YouTube-Videos und Instagram-Fotos wurden von der Webseite gesammelt.

Seit Netzpolitik begonnen hat, *kritische Fragen* zu stellen, bewirbt die Firma ihre Dienste als Privatsphäre-Schutz, der ausschließlich die Suche nach eigenen Fotos erlauben soll. Zuvor schlug die Firma Nutzer*innen noch explizit vor, fremde Bilder, etwa von Prominenten, zu suchen. Einen effektiven Schutz gibt es bis heute nicht, der verhindern könnte, dass die Suchmaschine für Stalking oder Überwachung von Mitarbeiter*innen missbraucht wird.

Dass PimEyes nicht ausschließlich zur Suche nach dem eigenen Bild gedacht ist, zeigt sein Geschäftsmodell, basierend auf kostenpflichtigen Premium-Funktionen, die etwa ein Sonderangebot für 100 Millionen Datenbankabfragen pro Monat enthalten.

Der Datenschutzbeauftragte für Baden-Württemberg, Stefan Brink, geht davon aus, dass PimEyes gegen die Datenschutz-Grundverordnung verstößt. Da es sich bei biometrischen Daten um besonders schutzwürdige Informationen handelt, hätte die Firma von jeder Person in ihrer Datenbank aus 900 Millionen Gesichtern eine Einwilligung einholen müssen. Dennoch ist es möglich, dass PimEyes schon heute von europäischen Behörden genutzt wird. Der Firma ist nämlich der Coup gelungen, eine Kooperation mit dem schwedischen Unternehmen Safer Society einzugehen, das seinerseits PimEyes in seine Überwachungssoftware Paliscope integriert hat, die es Behörden zur staatlichen Überwachung oder Strafverfolgung anbietet. Auch die europäische Polizeibehörde Europol ist Kundin von Safer Society.

## EU-Kommission will Gesichtserkennung nicht bekämpfen

Als Kommissionspräsidentin Ursula von der Leyen ins Amt gewählt wurde, versprachen sich manche ein härteres Durchgreifen gegen Gesichtserkennungs-Technologien. Von der Leyen versprach einen Gesetzesvorschlag zur Regulierung der „künstlichen Intelligenz" innerhalb von 100 Tagen (die inzwischen bereits verstrichen sind). Kern der europäischen KI-Regulierung sollten hohe ethische Standards sein, die das Vertrauen in die Technologie stärken und den Vorzug gegenüber rein wirtschaftlichen Erwägungen bekommen sollten.

Ein solcher Gesetzesvorschlag ist bislang ausgeblieben. Anfang des Jahres hat die EU-Kommission lediglich ein Strategiepapier zur künstlichen Intelligenz veröffentlicht. Eine Passage, die in einer früheren Entwurfsfassung ein zeitweises Verbot von Gesichtserkennung im öffentlichen Raum vorschlug, wurde aus der Endfassung gestrichen.

## EU-Kommission investiert in KI-Lügendetektor

Welche ethischen Standards die EU-Kommission tatsächlich an Gesichtserkennung anlegt, sieht man derweil an ihren Förderprojekten: Aus dem EU-Forschungsfördertopf Horizon 2020 *finanziert sie seit Jahren das Programm iBorderCTRL*. Hinter dem Programm mit dem dystopischen Namen steckt nichts anderes als ein Lügendetektor, der Menschen bei Grenzübergängen mittels biometrischer Daten vom Gesicht ablesen soll, ob sie in Verhören die Wahrheit sagen.

Dass Lügendetektoren auf Pseudowissenschaft basieren und Gesichtserkennungstechnik insbesondere bei nicht-weißen Menschen erhebliche Fehlerquoten aufweist, hat die EU nicht davon abgehalten, das Programm an den EU-Außengrenzen zu testen, woraufhin Journalist*innen von The Intercept *prompt solche Fehler durch iBorderCTRL nachweisen konnten*. Dem EU-Abgeordneten Patrick Breyer *verweigert die EU-Kommission Informationen* über die grundrechtliche Evaluation und die Fehlerraten von iBorderCTRL.

## Gesichtserkennung auch in Deutschland

Auch deutsche Behörden setzen vermehrt Gesichtserkennung ein. Die *Anzahl der Abfragen von Gesichtserkennungsdatenbanken durch Bundespolizei und Kriminalämter* nimmt rasant zu. Dennoch ist in Deutschland und Europa bislang eine breite gesellschaftliche Debatte darüber ausgeblieben, wie die immer weitere Verbreitung von

Gesichtserkennung im Alltag nicht nur zu falschen Verdächtigungen beitragen kann, sondern auch unser Verhalten im öffentlichen Raum beeinflusst.

Das Gefühl, unter ständiger Beobachtung zu stehen, löst Stress aus und führt zu einem angepassten Verhalten. Wer befürchten muss, dass bei einer Teilnahme an Demonstrationen Gesichter abfotografiert und von der Polizei – oder sogar von Neonazis – mittels Gesichtserkennung zur Enttarnung von Demonstrierenden genutzt werden, wird sich zweimal überlegen, ob die Wahrnehmung des Grundrechts auf Versammlungsfreiheit das Risiko wert ist.

Das ist keine rein theoretische Gefahr: Bei den G20-Protesten in Hamburg hat die Polizei eine umfangreiche *Datenbank zur automatischen Gesichtserkennung* angelegt. Bei Tests der Software PimEyes durch das *Investigativteam von Netzpolitik* fand dieses unter anderem auch Fotos der Bundestagsabgeordneten Anke Domscheit-Berg bei der Teilnahme an einer Anti-Überwachungs-Demo. Das Missbrauchspotential von immer größeren, verdachtsunabhängigen Datensammlungen, die sowohl von Behörden als auch von Unternehmen zur Gesichtserkennung genutzt werden, ist also erheblich.

**Aufstand gegen Gesichtserkennung in den USA**

In den USA ist der Einsatz von Gesichtserkennung zwar bereits weiter fortgeschritten als in Europa. So setzen Strafverfolgungsbehörden die *Gesichtserkennungs-Datenbank des umstrittenen Unternehmens Clearview AI* ein. Doch auch der Widerstand aus Zivilgesellschaft und Wissenschaft ist deutlich lauter – und zeigt erste Ergebnisse.

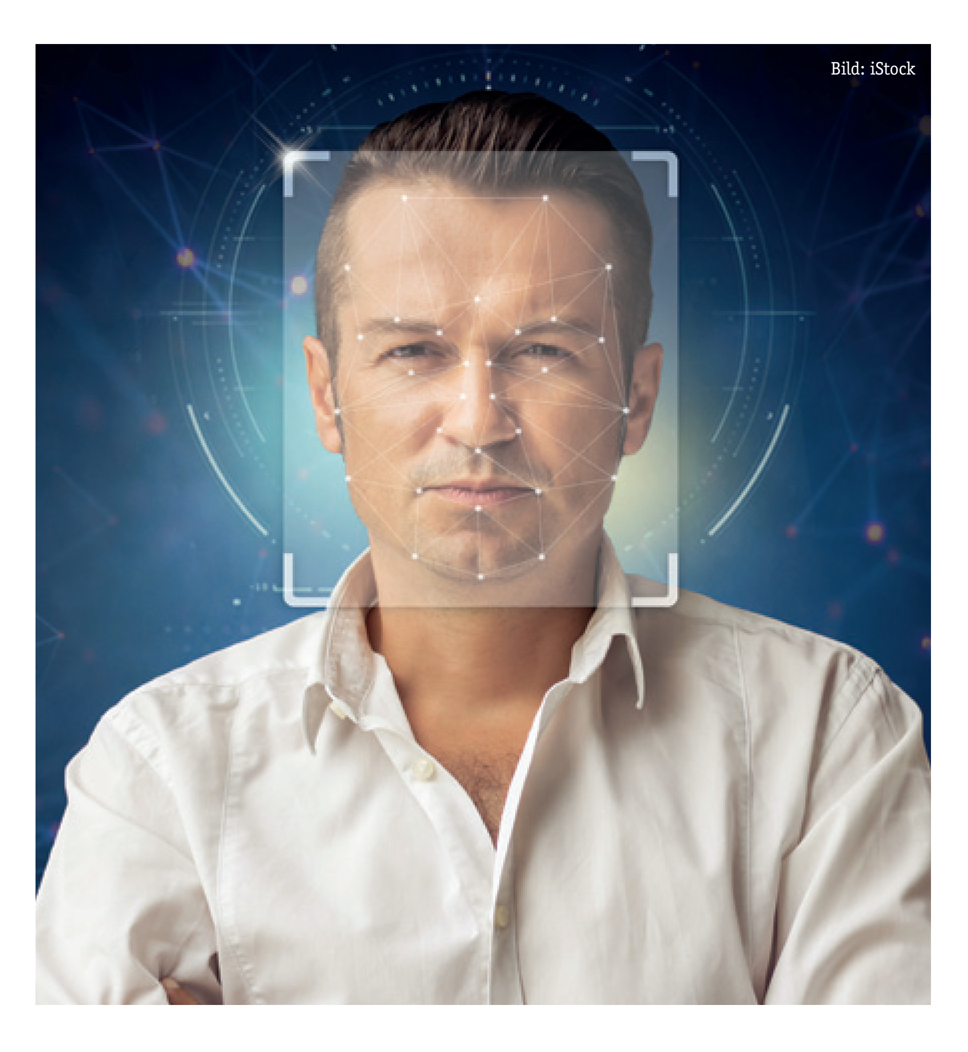
Studien über die diskriminierende Wirkung von Gesichtserkennung, die bei den Gesichtern von Frauen und nicht-weißen Personen sehr viel höhere Fehlerraten produziert als bei weißen Männern, haben die Technologie in Verruf gebracht. Pionierarbeit hat hierbei die Wissenschaftlerin Joy Buolamwini geleistet, *deren Studie „Gender Shades" das Phänomen bereits 2018 nachgewiesen hat* und deren Ergebnisse seitdem mehrfach von renommierten Wissenschaftseinrichtungen reproduziert wurden. Buolamwini gründete die Algorithmic Justice League, eine zivilgesellschaftliche Initiative gegen den Einsatz diskriminierender Technologien. Als es dann tatsächlich zur falschen Festnahme des Afroamerikaners Robert Williams durch Fehler bei der Gesichtserkennung kam, war das Problem durch die Vorarbeit von Wissenschaft und Zivilgesellschaft der Presse bereits bekannt. Der Fall machte landesweit Schlagzeilen. Auch der Talkshow-Host *John Oliver hat die Gefahren von Gesichtserkennung in einem Video aufgegriffen*, das allein auf YouTube bereits sieben Millionen Mal gesehen wurde.

**Der Aufstand lohnt sich**

Die Kampagne gegen Gesichtserkennung in den USA hat bereits eine Reihe von Erfolgen vorzuweisen. Mehrere Städte, darunter San Francisco und Oakland, haben die Gesichtserkennung im öffentlichen Raum verboten. Der Bundesstaat Massachusetts berät das Verbot, das mehrere Gemeinden dort bereits beschlossen haben, auf den gesamten Staat auszuweiten. Infolge der Black Lives Matter-Proteste, die Rassismus und Polizeigewalt in den Fokus genommen haben, *entzogen Microsoft, Amazon und IBM* der US-Polizei (zumindest vorübergehend) den Zugang zu ihren Gesichtserkennungs-Tools.

Dieses Engagement brauchen wir auch in Deutschland und Europa, um der rasanten Ausbreitung und Normalisierung von Gesichtserkennung etwas entgegenzusetzen. In der Initiative *Gesichtserkennung Stoppen!* haben sich unter anderem der *Chaos Computer Club, D64 – Zentrum für digitalen Fortschritt* (dessen Beirat ich angehöre) und *Digitale Gesellschaft e.V.* zusammengeschlossen, um ein Verbot von Gesichtserkennung im öffentlichen Raum und dessen Einsatz durch den Staat zu erreichen.




Bild: iStock

Friedemann Ebelt

# Fingerabdrücke im Personalausweis – was tun? #PersoOhneFinger

Ab 2. August 2021 wird die Speicherung von Fingerabdrücken auf Personalausweisen zum Zwang: Trotz Kritik von Datenschutz- und Grundrechteorganisationen haben die Regierungen der EU-Länder und eine knappe Mehrheit im EU-Parlament 2019 eine Verordnung zur Erhöhung der Sicherheit der Personalausweise und der Aufenthaltsdokumente beschlossen. Ein deutsches Gesetz zur Umsetzung ist bereits in Arbeit. Dieses zwingt ab 2. August 2021 anlasslos alle Menschen, einen Abdruck ihres linken und rechten Zeigefingers abzugeben. So werden Millionen rechtskonformer Menschen behandelt wie Tatverdächtige. Wir halten das für undemokratisch und raten:

Alle Menschen, die einen Personalausweis ohne Fingerabdrücke wollen, sollten bis zum Beginn der Speicherpflicht einen Personalausweis ohne Fingerabdrücke beantragen. Bitte werdet auch politisch gegen das Gesetz aktiv! Mehr dazu unter: Jetzt aktiv werden. #PersoOhneFinger

## Angriff auf die Würde des Menschen

Digitalcourage sieht mit dieser Verordnung die Würde aller betroffenen Menschen angegriffen und bewertet das Gesetz als grundrechtswidrig. Die zwangsweise und anlasslose Abgabe von biometrischen Daten entspricht nicht den Werten von Rechtsstaaten und Demokratien, sondern der Kontrollsucht von Polizeistaaten.

## Die Rechtslage

In Deutschland war die Abgabe von Fingerabdrücken für den Personalausweis bislang freiwillig. (Verpflichtend ist die Abgabe aber bereits für Reisepässe.) Bürgerinnen und Bürger können derzeit noch wählen, ob ihr neuer Personalausweis Fingerabdrücke enthalten soll oder nicht. In der Praxis werden die




Menschen aber häufig nicht über die Freiwilligkeit und die Konsequenzen der Fingerabdrücke aufgeklärt. Viele Menschen werden im Moment der Antragstellung kurzerhand zur Abgabe ihrer Fingerabdrücke verleitet.

**Ab 2. August 2021 wird die freiwillige Abgabe zum Zwang:** Ab dann werden die Fingerabdrücke lokal auf einem Chip in den Personalausweisen gespeichert. Die EU-Verordnung 2019/1157, die die Fingerabdruckpflicht enthält, wurde 2019 mit Stimmen aus Deutschland beschlossen. Mit dem Gesetz zur Stärkung der Sicherheit im Pass-, Ausweis- und ausländerrechtlichen Dokumentenwesen (siehe auf bmi.bund.de) wird das deutsche Personalausweisgesetz entsprechend angepasst. Wer derzeit einen gültigen Personalausweis besitzt, kann diesen bis zum Ablauf der angegebenen Gültigkeit nutzen – es besteht keine Pflicht, ab dem 2. August 2021 einen Ausweis mit Fingerabdrücken zu beantragen. Wir empfehlen deshalb, vor dem 2. August 2021 einen Personalausweis ohne Fingerabdrücke zu beantragen, um diesen 10 Jahre nutzen zu können, mehr unter: aktiv werden.

Hinweis: Wenn aufgrund von Abnutzung der Fingerkuppen oder Verletzungen keine Abdrücke genommen werden können, werden für 12 Monate Personalausweise ohne Fingerabdrücke ausgestellt:

Das Thema steht für den 10. September 2020 auf der Tagesordnung des Bundestags, siehe bundestag.de. Das kann sich allerdings kurzfristig ändern.

*„Artikel 4: (3) Die Mitgliedstaaten stellen einen Personalausweis mit einer Gültigkeitsdauer von zwölf Monaten oder weniger aus, wenn vorübergehend aus physischen Gründen von keinem der Finger Fingerabdrücke genommen werden können. (siehe Seite 8 der Verordnung auf eur-lex.europa.eu)“*

**Gut zu wissen:** Zuständig für Fragen zum Personalausweis ist der Bürgerservice des Bundesinnenministeriums personalausweisportal.de:

Die telefonische Servicehotline ist von 08:00-16:30 Uhr erreichbar.

Gebühren: 3,9 ct/Min. aus dem deutschen Festnetz, aus dem Mobilfunknetz max. 42 ct/Min., auch aus dem Ausland erreichbar, Telefon: 0180-1-33 33 33
E-Mail: eID_buergerservice@bmi.bund.de

## Warum Fingerabdrücke ein Problem sind

Die Pflicht zur Abgabe von Fingerabdrücken ist aus unserer Sicht ein Fehler, weil sie politische, technische, grundrechtliche und ethische Gefahren enthält, aber keine Probleme löst.

- Lebenslange Kontrolle: Ein Fingerabdruck ist ein biometrisches Merkmal, welches einen Menschen ein Leben lang kontrollierbar macht. Menschen können, wenn es sein muss, Namen und Wohnort wechseln, um sich beispielsweise vor Verfolgung oder Bedrohung zu schützen. Biometrische Daten wie Fingerabdrücke erlauben das nicht.
- Übergriff statt Schutz: Die anlasslose und massenhafte biometrische Erfassung von Fingerabdrücken ist ein nutzloser und gefährlicher Übergriff des Staats auf die Bevölkerung. Demokratien und Rechtsstaaten haben die Aufgabe, Bürgerinnen und Bürger vor derartigen Übergriffen zu schützen.
- Freiheit wird schrittweise abgeschafft: Überwachungs- und Kontrollmaßnahmen werden stets erweitert

und verschärft, aber so gut wie nie zurückgefahren. Ohne politischen Kurswechsel werden in Zukunft immer mehr Arten sensibler Biometriedaten millionenfach erhoben, gespeichert und für alle möglichen Zwecke genutzt.

- Risiko Zugriffserweiterung: In Deutschland dürfen Polizei und Geheimdienste seit 2017 automatisch auf biometrische Passbilder von Personalausweisen zugreifen. Dabei gibt es wenig Kontrolle durch Aufsichtsbehörden. Eine Ausweitung der Zugriffsmöglichkeiten auf die Fingerabdrücke scheint nur eine Frage der Zeit.
- Kontrollverlust durch Drittstaaten: Durch „weltweite Interoperabilität – auch bei der Maschinenlesbarkeit und der Sichtprüfung“ (Erwägungsgrund Nr. 23) können die biometrischen Daten auch an Behörden in Staaten, in denen Freiheitsrechte nicht geschützt sind, gelangen. Spätestens hier gibt es keine Kontrolle darüber, wohin die biometrischen Daten der Bürgerinnen und Bürger gelangen.
- Kontrollverlust durch Unternehmen: Bei „Zusammenarbeit mit einem externen Dienstleistungsanbieter“ (Erwägungsgrund Nr. 42) können auch private Unternehmen Zugriff auf die Daten erhalten, siehe auch Artikel 11 „Schutz personenbezogener Daten und Haftung“.
- Kontrollverlust durch Geheimdienste: Nach den Enthüllungen von Edward Snowden haben es die Regierungen der EU-Länder versäumt, die Macht von Geheimdiensten wirksam einzuschränken. Im NSU-Skandal hat der mit einem BigBrotherAward für sein Lebenswerk ausgezeichnete sogenannte deutsche „Verfassungsschutz“ die Aufklärung von Terror behindert. Geheimdienste arbeiten unkontrolliert und grundrechtefeindlich. Es muss davon ausgegangen werden, dass Geheimdienste sich unkontrolliert Zugriff auf die biometrischen Daten der EU-Bürgerinnen und -Bürger verschaffen werden.
- Risiko Datenvernetzung: Bereits jetzt arbeiten „Sicherheits“-Politiker.innen an einer vernetzten, EU-weiten Datenbankstruktur mit Fingerabdrücken, Gesichtsbildern und anderen Biometriedaten, siehe netzpolitik.org vom 17. Juli 2020 und unseren Text zu diesem Thema. Datenbanken von Verwaltungen, Polizei, Geheimdiensten und Firmen wachsen ständig. (siehe Programme: Next Generation Prüm, Polizei 2020, Ausbau des Visa-Informations-Systems oder des Schengener-Informations-Systems SIS II).
- Kinder betroffen: Laut EU-Verordnung werden Kinder ab 6 Jahren erfasst, wobei die einzelnen Regierungen der EU-Ländern die Möglichkeit haben, Kinder bis 12 Jahren von der Pflicht zur Abgabe von Fingerabdrücken zu befreien.
- Illegitim in Demokratien: Ralf Bendrath erläutert in seinem Beitrag „Zur Geschichte der Fingerabdrücke in Ausweisen“: „Ausweise gehen in Deutschland auf die von den Nazis ab 1938 eingeführte „Kennkarte“ zurück, deren Mitführen für Juden zwingend war. (...) In Spanien wurde die Erfassung von Fingerabdrücken für die nationale Identitätskarte, die bis heute gilt, 1940 während der Franco-Diktatur eingeführt. Was nun allen BürgerInnen aufgenötigt wird, steht also ganz klar in der Tradition verbrecherischer Regime.“ In Frankreich nutzte das Vichy-Regime ab 1942 den Eintrag Jude auf Ausweisen für die Deportation von 76.000 Menschen im Holocaust (mehr dazu auf lto.de vom 22.7.2018: 80 Jahre Ausweispflicht: Wie ein Nazi-Minister den Überwachungsstaat durchsetzte).
- Datensicherheit: Die Daten der gespeicherten Fingerabdrücke auf den neuen Personalausweisen können kontaktlos ausgelesen werden. Ein Speichermedium, das heute nicht geknackt werden kann, kann möglicherweise in 10 Jahren geknackt werden.

Schon lange träumen vermeintliche Sicherheitspolitiker.innen in der EU von einer biometrischen Superdatenbank, wir informieren über die Pläne.

**Jetzt aktiv werden!**

Juristisches Vorgehen gegen die EU-Fingerabdruckpflicht ist aufgrund der geltenden Klagebefugnisse auf europäischer Ebene schwierig. **Aber: Es kann einiges gegen das deutsche Umsetzungsgesetz getan werden, das vermutlich im Herbst 2020 im Bundestag diskutiert wird.**

Wir raten allen Menschen, die einen Personalausweis ohne Fingerabdrücke wollen, bis zum Beginn der Speicherpflicht ein fingerabdruckfreies Dokument zu beantragen.

Aber: Neue Personalausweise gelten maximal 10 Jahre. Darum ist es notwendig auch **politisch aktiv zu werden** und die Gesetze auf EU- und Bundesebene dauerhaft zu ändern. Dazu gibt es folgende Möglichkeiten:

**1. Schreibe deine Bundestagsabgeordneten an** und erkläre deine Kritik an der Pflicht für Fingerabdrücke in den neuen Personalausweisen. Fordere zum Beispiel, dass sie sich gegen das deutsche Umsetzungsgesetz aussprechen und dagegen stimmen. Die Pflicht steckt im Entwurf des Gesetzes zur Stärkung der Sicherheit im Pass-, Ausweis- und ausländerrechtlichen Dokumentenwesen, siehe auf bmi.bund.de. Derzeit steht das Thema für den 10. September 2020 auf der Tagesordnung im Bundestag. Auf bundestag.de ist eine, nach Bundesland, PLZ und Wahlkreis sortierbare, Liste mit Kontakten der Abgeordneten.

Wichtig zu wissen: Weil die Grundlage für die Fingerabdruck-Pflicht eine EU-Verordnung ist, an die die deutschen Gesetze nur angepasst werden, ist es leider unwahrscheinlich, dass der Bundestag den Mut aufbringen wird, den Kurs zu ändern. Trotzdem muss unserer Ansicht nach dieses Gesetz auf laute Kritik und breite Ablehnung aus der Bevölkerung treffen.

Primär sind die Regierungen der EU-Länder und die Abgeordneten im EU-Parlament verantwortlich. Wer 2019 wie abstimmt hat, haben wir in der Info-Box verlinkt. Eine durchsuchbare Übersicht aller deutschen EU-Abgeordneten gibt es auf auf der Website des EU-Parlaments, auch sortiert nach Bundesländern.

**2. Hilf, diese Informationen zu verbreiten,** via E-Mail, Websiten, Messenger-Gruppen und in Sozialen Medien: **#PersoOhneFinger**

**3. Wähle keine Überwachungsparteien.**

**Eine Bitte:** Teile uns gern mit, was du getan und welche Reaktionen du bekommen hast. E-Mail an: mail+persoohnefinger@digitalcourage.de oder im Fediverse oder auf Twitter: **#PersoOhneFinger**

### Hintergrund: Es geht nicht um Sicherheit

Begründet wurde die Verordnung (EU) 2019/1157 mit Sicherheit, *„insbesondere im Zusammenhang mit Terrorismus und grenzüberschreitender Kriminalität.“* (siehe Erwägung Nr. 6). Aus Sicherheitsgründen soll die Pflicht zur Abgabe von Fingerabdrücken die Personalausweise fälschungssicherer machen.

Allerdings ist aufgrund der technischen Verbesserung der Merkmale die Zahl von gefälschten Dokumenten stark rückläufig, so die EU-Grenzagentur Frontex, (siehe PDF auf frontex.europa.eu S. 22). Der Nutzen der Verordnung zur Verhinderung von Terrorismus ist nicht nachgewiesen. Die Untersuchungen der NSU-Morde und des Terroranschlags von Anis Amri haben ergeben, dass die Täter behördlich bekannt waren. Fehlende Daten, fehlende Überwachungs- und Identifizierungsmöglichkeiten waren nicht das Problem für die Ermittlungsbehörden. Erläutert hat das Sascha Lobo in dem Text Klare Zahlen gegen Massenüberwachung auf netzpolitik.org.

Die millionenfache Abgabe von Fingerabdrücken von rechtstreuen Bürgerinnen und Bürgern ist nicht nötig und nicht verhältnismäßig.

Unserer Einschätzung nach handelt es sich bei der Verordnung (EU) 2019/1157 um Sicherheitstheater zum Nachteil der Bevölkerung.

Eine Politik, die Freiheit angreift und scheibchenweise verhökert, verdient nicht „Sicherheitspolitik“ genannt zu werden. … Wir brauchen echte Sicherheitspolitik, die uns auch wirklich sicherer macht, anstatt uns zu bedrohen (mehr zu Sicherheitstheater bei Digitalcourage).

Die Bundesregierung hat 2019 im Rat der Europäischen Union für Fingerabdruckpflicht gestimmt. Die Regierungen der Slowakei und Tschechien haben gegen die Verordnung gestimmt. Letztere hat die verpflichtende Abgabe für alle Menschen als unverhältnismäßig bewertet, siehe votewatch.eu.

Ergänzung vom 4. August 2020: Wer rechtzeitig einen Personalausweis ohne Fingerabdrücke beantragen möchte, sollte beachten, dass es bei Bürgerämtern/Bürgerservices durchaus mehr als sechs Wochen dauern kann, um einen Termin zur Beantragung eines #PersoOhneFinger zu bekommen. Also: rechtzeitig kümmern! Und: Wer einen noch länger gültigen Personalausweis besitzt, kann einen neuen nur beantragen, wenn der alte beschädigt oder verloren ist; beziehungsweise mit berechtigtem Interesse nach Personalausweisgesetz §6 (2), siehe gesetze-im-internet.de, eine Seite des Justizministeriums.

Ergänzung vom 7. August 2020: Als Reaktion auf #PersoOhneFinger schreiben uns Menschen, dass Bürgerämter seit Jahren auf die Abgabe von Fingerabdrücken bestehen, obwohl das noch bis 2. August 2021 freiwillig ist! Wir raten:

1. schriftlich beim Bürgeramt beschweren
2. schriftlich beim Bürgerservice des Bundesinnenministeriums beschweren: eID_buergerservice@bmi.bund.de
3. einen Personalausweis ohne Fingerabdrücke (kurz: #PersoOhneFinger) beantragen
4. diesen Artikel via E-Mail, E-Mailinglisten oder in sozialen Medien verbreiten, Tweet / Tröt teilen

Uns interessieren die Reaktionen und Antworten von Behörden. Gern E-Mail an: mail+persoohnefinger@digitalcourage.de oder #PersoOhneFinger im Fediverse oder auf Twitter.

Auch (ggf. aktualisiert) zu finden unter: https://digitalcourage.de/blog/2020/keine-fingerabdruecke-personalausweis-persoohnefinger

## Klarstellung: Für Betriebsärzte gilt das Patientengeheimnis

In der DANA 1/2020 wurde auf S. 37 die Pressemitteilung des „Arbeitsbündnisses gegen Datenmissbrauch in der Medizin“ vom 01.12.2019 veröffentlicht, wonach ein Verband der Betriebsärzte, die Deutsche Gesellschaft für Arbeitsmedizin und Umweltmedizin (DGAUM) die Regierung aufgefordert habe „Einblick in die Gesundheitscloud“ zu geben. Tatsächlich forderte DGAUM erneut in einer Presseerklärung vom 19.05.2020 anlässlich ihrer Stellungnahme zum Entwurf eines Patientendaten-Schutzgesetzes (PDSG): „Die medizinische Versorgung durch Betriebsärzte ist ohne deren Zugang zur elektronischen Patientenakte nicht möglich“. Falsch ist die Behauptung der Pressemitteilung des Arbeitsbündnisses: „Damit werden Einstellungs- und Weiterbeschäftigungsuntersuchungen zum ‚Kinderspiel‘ – der Arbeitgeber kann alle Krankheiten des Arbeitnehmers lückenlos erfahren.“ Den Betriebsärzten geht es darum, die „Schnittstelle zwischen arbeitsmedizinischer und vertragsärztlicher Versorgung“ zu verbessern. Dies bedeutet jedoch nicht, dass damit die ärztliche Schweigepflicht aufgehoben werden soll. Auch der (betriebs-)ärztliche Zugriff auf die Daten der elektronischen Patientenakte setzt die Zustimmung des Patienten voraus. Völlig falsch ist die Aussage des Arbeitsbündnisses, dass mit einem Zugriff der Betriebsärzte die Arbeitgeber „alle Krankheiten des Arbeitnehmers lückenlos erfahren“ könne. Der Betriebsarzt unterliegt auch gegenüber dem Arbeitgeber der ärztlichen Schweigepflicht. Hieran soll sich gesetzlich auch nichts ändern.

Die DANA-Redaktion veröffentlicht natürlich Presseerklärungen unverändert. Falschbehauptungen sind den Autoren zuzuschreiben. Es mag nötig sein, diese künftig zu kommentieren.

Die DANA-Redaktion

# Datenschutznachrichten

## Datenschutznachrichten aus Deutschland

### Bund

### Gesundheitsminister beschließen Reise-Corona-Tests und Testpflicht

Die Gesundheitsminister von Bund und Ländern haben am 24.07.2020 in Bonn Corona-Testzentren an allen deutschen Flughäfen beschlossen. Die Kosten für diese Tests sollen übernommen werden. Wer aus einem Risikogebiet nach Deutschland zurückreist, soll sich künftig am Flughafen freiwillig kostenlos testen lassen können. Sonst gilt ohne negativen Befund weiterhin Quarantänepflicht. Beschlossen wurden folgende Kernpunkte:

- In allen deutschen Flughäfen mit relevantem Reiseverkehr werden Teststellen eingerichtet.
- Die Bundespolizei weist Reisende aus Risikogebieten auf die Teststellen hin.
- Auch Rückreisende aus Nichtrisikoländern können sich außerhalb der Flughäfen testen lassen.
- Die Kosten für sämtliche Tests für Rückreisende sollen durch die Krankenkassen und die Bundesländer übernommen werden.

Weiterhin blieben die Beschlüsse bestehen, dass Menschen, die aus Risikoländern einreisen, zu einer 14-tägigen Quarantäne verpflichtet sind und die Quarantäne nur mit einem negativen Testbefund beendet werden kann.

Die Gesundheitsminister stellten fest, dass Infektionsketten „in beachtlicher Anzahl auf Reiserückkehrende zurückzuführen“ sind, so die Berliner Gesundheitssenatorin Dilek Kalayci (SPD). Die Nationale Teststrategie werde deshalb so ergänzt, dass sich alle Reiserückkehrer binnen drei Tagen nach Einreise testen lassen können. Für Einreisende aus Risikogebieten sollen die Tests direkt an den Flughäfen angeboten werden.

Vor dem Treffen hatten sich Sachsens Ministerpräsident Michael Kretschmer (CDU) und Bayerns Ministerpräsident Markus Söder (CSU) für verpflichtende Tests stark gemacht, konnten sich damit aber nicht durchsetzen. Anlass für Diskussionen hatten Partys auf Mallorca gegeben, bei denen Urlauber weder Masken trugen noch Abstand hielten. Das Robert-Koch-Institut (RKI) hat weltweit mehr als 100 Staaten als Gebiete eingestuft, in denen ein erhöhtes Risiko für eine Infektion mit dem Coronavirus besteht, dazu gehören derzeit unter anderem die Reiseländer Ägypten, Israel, die Türkei, Südafrika und die USA.

Schleswig-Holsteins Bildungsministerin Karin Prien hatte zuvor Lehrer vor Auslandsreisen in Risikogebiete gewarnt. Wenn sie anschließend in Quarantäne müssten und deshalb den Schulstart verpassten, werde dies als unberechtigtes Fernbleiben betrachtet. In der Folge würden Dienstbezüge einbehalten, tariflich Beschäftigten drohe zudem eine Abmahnung. Schüler und deren Eltern mahnte sie, mit Reisen in Risikogebiete unter Umständen eine Ordnungswidrigkeit zu begehen, „die mit einer Geldbuße geahndet werden kann“.

Schon seit Ende Juni, Anfang Juli 2020 waren an einigen deutschen Flughäfen Testzentren für Reisende eingerichtet worden. Das sind teils privatwirtschaftliche Kooperationen wie etwa am Frankfurter Flughafen, wo das Unternehmen Centogene zusammen mit Betreiber Fraport und der Lufthansa ein kommerzielles Testzentrum anbietet. Am Flughafen Köln-Bonn sind die Johanniter im Auftrag der Stadt Köln mit einem mobilen Testzentrum für freiwillige Tests präsent. Die Arbeitsgemeinschaft Deutscher Verkehrsflughäfen betonte, dass die Mitarbeiter der Flughäfen nicht befugt sind, Passagiere auf ihren Gesundheitsstatus hin zu überprüfen. In jedem Fall gilt: Sollten die Gesundheitsbehörden einen Schnelltest anordnen, müsste dieser von den Behörden selbst durchgeführt werden.

Am Frankfurter Flughafen hatten die Tests zunächst je nach Wartezeit 59 Euro beziehungsweise 139 Euro gekostet, in München 190 Euro. Viele dieser Tests wurden für Reisende durchgeführt, die von diesen Flughäfen abfliegen, um zu verhindern, dass sie sich am Ziel in Quarantäne begeben müssen. Manche Airlines ließen nur Passagiere an Bord, die einen negativen Test vorlegen konnten.

Peter Bauer von Centogene erklärte Ende Juli: „Wir haben vom Start weg festgestellt, dass es einen hohen Bedarf gibt. Aktuell sind es über tausend Menschen, die täglich unser Angebot am Frankfurter Flughafen nutzen.“ Auf steigende Passagierzahlen sei man vorbereitet. „Mit unseren Laborkapazitäten vor Ort sind bis zu 12.000 Proben täglich analysierbar.“ Bislang bewegte sich der Anteil der positiven Corona-Tests am Frankfurter Flughafen im „mittleren Promillebereich“. An den Standorten hatte es zuvor jeweils Verhandlungen zwischen Testanbietern, Flughafenbetreibern und Gesundheitsbehörden über die Einrichtung der Testzentren gegeben.

Nicht nur für Flugreisende aus dem Ausland, sondern auch für den grenzüberschreitenden Verkehr mit Schiff, Bus und Bahn wurden gemäß Senatorin Kalayci Aussteigekarten eingeführt. Wer aus einem Risikogebiet nach Deutschland kommt, muss ein solches Formular ausfüllen und abgeben. Außerdem verständigten sich die Gesundheitsminister darauf, dass „in grenznahen Einreisepunkten“ des Straßenverkehrs „stichprobenartige Kontrollen“ durchgeführt werden. Wenn dabei herauskomme, dass jemand aus einem Corona-Risikogebiet komme, werde er auf die Quarantänepflicht hingewiesen.

Direkt darauf kündigte Gesundheitsminister Jens Spahn (CDU) eine Verordnung auf Grundlage des Infektionsschutzgesetzes an, wonach Einreisende aus Corona-Risikogebieten verpflichtet werden, sich auf das Virus testen zu lassen: „Wir müssen verhindern, dass

Reiserückkehrer unbemerkt andere anstecken und so neue Infektionsketten auslösen. Das dient dem Schutz aller Bürgerinnen und Bürger." Zuvor waren die Rufe nach einer Testpflicht immer lauter geworden. So hatte z.B. Bayerns Ministerpräsident Markus Söder (CSU) eine entsprechende Regelung gefordert und sich zugleich dafür ausgesprochen, die Risikogebiete noch einmal neu zu überprüfen. Die Pflichttests sind gemäß den Vorgaben des Bundesgesundheitsministeriums kostenlos. Der nordrhein-westfälische Gesundheitsminister Karl-Josef Laumann hatte dagegen zuvor noch betont, die Kosten sollten „von denjenigen, die meinten, in Risikogebieten Urlaub machen zu müssen, selber getragen werden" (Stadler, Corona-Tests am Flughafen, SZ 23.07.2020, 6; Freiwillige Corona-Tests an allen Flughäfen, www.zdf.de 24.07.2020; Spahn will Testpflicht einführen, SZ 28.07.2020, 1).

**Bund**

## Flüchtlinge klagen gegen Smartphone-Auswertung

Mehrere Flüchtlinge haben gegen die Auswertung ihrer Handydaten durch das Bundesamt für Migration und Flüchtlinge (BAMF) Klage erhoben. Die Behörde missachte die hohen verfassungsrechtlichen Vorgaben, an die der Staat beim Zugriff auf persönliche Daten gebunden sei, meint die Gesellschaft für Freiheitsrechte (GFF), welche die Klagen unterstützt. Lea Beckmann von der GFF erläutert, die Auswertung der Handys durch das BAMF lasse „sehr umfassende Schlüsse über das Nutzungsverhalten eines Geflüchteten zu". Das Amt erlange Zugriff auf Kontakte, Rufnummern, Fotos, Apps, Adressen von Websites und E-Mail-Adressen. Geklagt gegen das Auslesen der Handydaten haben Flüchtlinge aus Afghanistan, Kamerun und Syrien. Die Klagen wurden bei den Verwaltungsgerichten in Berlin, Hannover und Stuttgart eingereicht.

Die Kläger führen auch an, dass sich das Instrument als „untauglich" erwiesen habe, da Handydaten aus technischen Gründen oftmals gar nicht ausgelesen werden könnten. In einer Klageschrift heiße es: „Anders als sonstige Beweismittel in Gerichtsverfahren kann die Qualität und Zuverlässigkeit der Datenträgerauswertung überhaupt nicht überprüft oder in Zweifel gezogen werden." Seit 2017 darf das Bundesamt per Gesetz die Handys von Asylbewerbern auswerten, wenn der Flüchtling sich bei der Asylbehörde nicht ausweisen kann, etwa durch einen Reisepass oder ein anderes Dokument.

Das Bundesinnenministerium nannte die Handy-Auswertung in diesen Fällen „die einzige oder jedenfalls eine wichtige Quelle für die Feststellung der Identität und Staatsangehörigkeit einer Person". Durch enge Vorgaben werde die Verhältnismäßigkeit des Eingriffs in die Persönlichkeitsrechte des Asylsuchenden gewahrt. Das BAMF hat eigenen Angaben zufolge zwischen Anfang 2019 und Ende April 2020 rund 11.756 Datenträger von Asylantragstellern ausgelesen und gespeichert. In gut 4.000 Fällen habe das Amt die Daten tatsächlich ausgewertet. In 60% der Fälle hätten sich „keine zusätzlichen Erkenntnisse" ergeben, die für das Asylverfahren relevant seien. In 38% der Fälle hätten die ausgewerteten Daten die Angaben des Geflüchteten bestätigt. In nur zwei Prozent der Fälle hätten die Analysen die Aussagen der Asylbewerber widerlegt (Flüchtlinge klagen gegen Auswertung ihrer Handydaten, www.zeit.de 05.05.2020).

**Bund**

## BSI soll mehr Personal und mehr Befugnisse erhalten

Bundesinnenminister Horst Seehofer (CSU) plant fest, das Bundesamt für die Sicherheit in der Informationstechnik (BSI) zu einer mächtigen Cyber-Behörde mit Hackerbefugnissen aufzurüsten. Gemäß einem überarbeiteten Referentenentwurf für ein 2. Gesetz „zur Erhöhung der Sicherheit informationstechnischer Systeme" soll das BSI mit 583 zusätzlichen Stellen zu einem wesentlichen Akteur im Kampf gegen Botnetze, vernachlässigte Geräte im Internet der Dinge oder Verbreiter von Schadsoftware werden.

Zur Abwehr „erheblicher Gefahren für die Kommunikationstechnik des Bundes", für eine kritische Infrastruktur oder für „die Verfügbarkeit von Informations- oder Kommunikationsdiensten" soll das BSI die Betreiber anweisen können, betroffene Anlagen von einem Schadprogramm zu „bereinigen". Das gilt auch, wenn es zu unerlaubten Zugriffen „auf eine Vielzahl von Telekommunikations- und Datenverarbeitungssystemen von Nutzern" kommt. Das BSI soll laut dem Entwurf auch „Portscans" durchführen dürfen sowie „Sinkholes" und „Honeypots" betreiben, um IT-Angreifern einfacher auf die Spur zu kommen.

Das BSI soll aktiv nach ungeschützten Netzen oder Systemen, die eine bereits bekannte Sicherheitslücke aufweisen oder die anderweitig angreifbar sind, suchen. Dies wäre etwa der Fall, wenn für ein System werkseitig stets ein identisches Passwort wie „0000" oder „admin" vergeben würde, so die Begründung. Um dies herauszufinden, müssten Mitarbeiter solche Kennungen ausprobieren, was bei Unbefugten bereits unter den Hackerparagrafen § 202 StGB wegen „Ausspähen von Daten" fallen könnte. Die Behörde soll „Protokolldaten" einschließlich personenbeziehbarer Nutzerinformationen wie IP-Adressen, die bei der Online-Kommunikation zwischen Bürgern und Verwaltungseinrichtungen des Bundes sowie Parlamentariern anfallen, für 18 Monate speichern und auswerten können. Dazu kommen interne „Protokollierungsdaten" aus sämtlichen Behörden in Form von Aufzeichnungen über die Nutzungsform von IT.

Die für Betreiber kritischer Infrastrukturen bereits geltenden Meldepflichten und Mindeststandards will das Ministerium auf Unternehmen ausdehnen, die „von besonderem öffentlichem Interesse sind", weil ihr „Ausfall oder ihre Beeinträchtigung zu erheblichen volkswirtschaftlichen Schäden, zu einer Gefährdung für die öffentliche Sicherheit" oder zu einer „Beeinträchtigung der wesentlichen Sicherheitsinteressen" des Landes führen könnten. Das Innenministerium nennt unter anderem „Rüstungshersteller sowie Hersteller von IT-Produkten für die Verarbeitung staatlicher Verschlusssachen".

Details will das Innenministerium per Rechtsverordnung festgelegen. Bei Verstößen gegen die Auflagen sollen

Bußgelder von bis zu 20 Millionen Euro oder vier Prozent des weltweit erzielten Jahresumsatzes drohen. Vorgesehen ist weiterhin eine „Huawei-Klausel". Von der Einführung eines im Kampf gegen Darknet-Betreiber umstrittenen Straftatbestands des „digitalen Hausfriedensbruchs" und des Doxxings steht in dem Entwurf nichts. Nutzern soll auch keine Beugehaft mehr drohen, wenn sie sich weigern Passwörter herauszugeben (Krempl, IT-Sicherheitsgesetz: BSI soll Daten 18 Monate auf Vorrat speichern, www.heise.de 12.05.2020, Kurzlink: https://heise.de/-4719797).

**Bund**

## MAD-Mitarbeiter verrät Dienstgeheimnisse

Nach Presserecherchen haben mindestens acht Soldaten des Kommandos Spezialkräfte (KSK) regelmäßig unberechtigerweise Ermittlungsinterna, also Dienstgeheimnisse, aus dem Militärischen Abschirmdienst (MAD) erhalten. Mindestens ein KSK-Mann, der die vertraulichen Informationen von einem Oberstleutnant des MAD erhalten hat, gab diese dann innerhalb der Truppe weiter. Der Bundeswehrgeheimdienst ermittelt selbst. Am 19.06.2020 wurden Parlamentarier in einer geheimen Sitzung informiert.

Ein Sprecher des MAD erklärte: „Bitte haben Sie dafür Verständnis, dass ich zu den laufenden Ermittlungen keine weiteren Angaben machen kann." Es würden umfangreiche Ermittlungen durchgeführt. Schließlich sei es von entscheidender Bedeutung, dass ein Amt, welches extremistische Umtriebe innerhalb der Truppe aufzuklären habe, absolut unangreifbar sein müsse. Ministerin Annegret Kramp-Karrenbauer sei entschieden, dies nun umfassend und schnell aufzuklären.

Dass ein MAD-Mitarbeiter offenbar Dienstgeheimnisse an einen befreundeten KSK-Soldaten verraten hatte, wurde am 18.06. bekannt. Dabei ging es um Ermittlungsergebnisse zum Fall des KSK-Soldaten Philipp Sch., der zuvor im Mai festgenommen worden war. In dessen Garten in Sachsen war ein privates Waffenversteck samt Sturmgewehr und Plastiksprengstoff entdeckt worden. Der MAD-Mitarbeiter soll Fotos der gefundenen Waffen einem anderen KSK-Angehörigen gezeigt und diesen gewarnt haben, der Bundeswehr-Geheimdienst könne sich möglicherweise auch für ihn interessieren. Der Oberstleutnant wurde suspendiert und soll keinen Zugang mehr zur Liegenschaft des Geheimdienstes haben. Es wird geprüft, ob diese Person auch weiteren KSK-Soldaten Informationen verraten hat.

Nach mehreren rechtsextremen Vorfällen im KSK hatte das Bundesverteidigungsministerium erklärt, die Eliteeinheit genauer in den Blick zu nehmen. Eine Arbeitsgruppe, zu der KSK-Kommandeur Markus Kreitmayr und Generalinspekteur Eberhard Zorn gehören und die von der neuen Wehrbeauftragen Eva Högl begleitet wird, soll bis Ende Juni einen Bericht dazu vorlegen. Dem KSK gehören mehr als 1.000 Soldaten an, die besonders gefährliche Mission im Ausland durchführen. Dazu gehören Anti-Terror-Einsätze in Afghanistan oder Geiselbefreiungen (Flade/ Mascolo/Steinke, Vertrauliches für die Freunde, SZ 20./21.06.2020, 6).

**Bund**

## Upskirting und Unfallgaffen werden Straftatbestände

Der Bundestag hat am 03.07.2020 ein Gesetz beschlossen, das eine Geldstrafe oder eine Freiheitsstrafe bis zu zwei Jahren für das sogenannte Upskirting vorsieht. Voraussichtlich ab Herbst ist damit das heimliche Fotografieren unter den Rock oder in den Brustausschnitt eine Straftat. Bundesjustizministerin Christine Lambrecht (SPD) erklärte, solche Grenzüberschreitungen seien nicht hinnehmbar. Die Fotos verletzten nicht nur die Persönlichkeitsrechte, sondern auch die sexuelle Selbstbestimmung: „Einer Frau unter den Rock oder in den Ausschnitt zu fotografieren, ist eine schamlose Verletzung ihrer Intimsphäre." Lambrecht hatte im September 2019 einen entsprechenden Gesetzentwurf angekündigt (DANA 4/2019, 217 f.). Bislang wurde das „Upskirting" meist nur als Ordnungswidrigkeit mit geringen Geldbußen geahndet. Das habe Täter nicht abgehalten, so der rechtspolitische Sprecher der SPD im Bundestag, Johannes Fechner: „Deshalb schließen wir hier eine wichtige Strafbarkeitslücke und verschärfen das Strafrecht an dieser Stelle."

Auch der rechtspolitische Sprecher des Koalitionspartners Jan-Marco Luczak (CDU) begrüßte das neue Gesetz: Das heimliche Fotografieren greife leider immer mehr um sich. „Wir steuern als Gesetzgeber jetzt entschlossen dagegen." Baden-Württembergs Justizminister Guido Wolf ergänzte: „Noch schlimmer ist es, wenn in der Folge solche Aufnahmen regelmäßig über das Internet einem unbegrenzten Kreis von Personen zugänglich gemacht werden."

Vor allem in großen Menschenmengen findet, so Nils Pickert von der feministischen Organisation Pinkstinks, Upskirting statt – in Bus und Bahn, auf Festivals, in Clubs und Bars: „Es gibt Leute, die verteilen winzige Kameras auf öffentlichen Toiletten, um damit Frauen abzufilmen." Auch das Downblousing sei weit verbreitet – das heimliche Fotografieren in den Ausschnitt: „Zum Beispiel wenn ich Ihnen auf einer gegenläufigen Rolltreppe entgegenkommen, so tue, als würde ich auf meinem Handy etwas lesen, in Wahrheit aber Ihre Brust fotografiere oder filme." Die 29jährige Hanna Seidel aus Ludwigsburg hatte zusammen mit Ida Marie Sassenberg aus München mit der Petition „Verbietet Upskirting in Deutschland!" die Debatte über das Thema in Gang gebracht und mehr als 100.000 Unterschriften gesammelt.

Baden-Württemberg, Bayern, Nordrhein-Westfalen und das Saarland hatten daraufhin eine Gesetzesinitiative im Bundesrat gestartet. Seidel meint ebenso wie Pickert, das Gesetz löse nicht gänzlich das Problem: „In der Gesellschaft muss noch viel passieren. Aber es ist ein richtiger und sehr wichtiger Schritt." Das Fotografieren im öffentlichen Raum gegen den Willen – insbesondere von Frauen – sei kein Kavaliersdelikt. „Es ist übergriffig, es ist eine Form von sexualisierter Gewalt und so muss man auch damit umgehen."

Die Essener Rechtsanwältin Jenny Lederer sieht das Gesetz dagegen kritisch: „Es gibt keine validen Zahlen, wie häufig dieses Problem vorkommt. Deshalb hat das Gesetz aus meiner Sicht nur Symbolcharakter. Ein einzelnes Phänomen ziel-

gerichtet als Straftatbestand auszugestalten, sei problematisch: „Strafrecht muss wirklich das letzte Mittel sein, um auf etwas Unerwünschtes zu reagieren.“

Das Gesetz zur „Verbesserung des Persönlichkeitsschutzes bei Bildaufnahmen“ zielt auch auf Gaffer an Unfallstellen ab. Das Fotografieren oder Filmen von Unfallopfern wurde ebenfalls zur Straftat erklärt. Wer, so Justizministerin Lambrecht, Schwerletzte oder gar Tote aus „reiner Sensationsgier fotografiert, verletzt jeden menschlichen Anstand.“ Bislang war ein solches Fotografieren von Verstorbenen nicht strafbar. Das Strafrecht schütze nur lebende Unfallopfer. Jenny Lederer: „Oft werden dabei auch noch Rettungskräfte behindert, die alles tun, um Leben zu retten.“ Auch diese Lücke werde jetzt geschlossen (Beschluss im Bundestag „Upskirting“ ist künftig Straftat, www.tagesschau.de 03.07.2020; REdan, Kampfansage gegen Spanner, KN 04.07.2020).

**Bund**

## Beirat für Beschäftigtendatenschutzgesetz

Am 16.06.2020 hat der interdisziplinäre Beirat zum Beschäftigtendatenschutz im Bundesministerium für Arbeit und Soziales (BMAS) seine Arbeit aufgenommen. Das aus 14 Personen bestehende Gremium unter Vorsitz von Prof. Herta Däubler-Gmelin, Bundesjustizministerin a.D., soll in den folgenden sechs Monaten Empfehlungen hinsichtlich der Notwendigkeit eines eigenständigen Gesetzes zum Beschäftigtendatenschutz erarbeiten. Das Gremium wird unter anderem beraten, ob und wie die Bundesregierung eine Öffnungsklausel in der Europäischen Datenschutzgrundverordnung nutzen sollte, um mit konkreten Regelungen den Beschäftigtendatenschutz in Deutschland transparenter und sicherer zu machen.

Bundesarbeitsminister Hubertus Heil erklärte dazu: „Wenn wir wettbewerbsfähig bleiben und einen Spitzenplatz in der Verwendung von neuen digitalen Anwendungen wie KI in Wirtschaft und Arbeitswelt einnehmen wollen, müssen wir dafür sorgen, dass die Beschäftigten diesen Technologien vertrauen. Sie müssen sich auch in Zukunft darauf verlassen können, dass ihre persönlichen Daten in ihrem Arbeitsumfeld gut geschützt sind. Ich freue mich, dass der Beirat zum Beschäftigtendatenschutz sich diesem wichtigen Thema annimmt. Denn der Weg in eine sozial gestaltete Datenökonomie kann nur gelingen, wenn die Perspektive der Beschäftigten konsequent beachtet und mitgedacht wird.“ Und die Vorsitzende Hertha Däubler-Gmelin ergänzte: „Die Mitglieder bringen Kenntnisse und Erfahrungen aus ganz unterschiedlichen Bereichen in die Arbeit des Beirats ein – gut für die dynamische Entwicklung der Arbeit in unserer Gesellschaft und den Beschäftigtendatenschutz!“

Dem Beirat, der von der Denkfabrik Digitale Arbeitsgesellschaft im BMAS koordiniert und begleitet wird, gehören folgende Expertinnen und Experten aus den Bereichen Technologie, Ethik und Arbeitspsychologie und Datenschutz an: Prof. Beate Bergmann, Bundesanstalt für Arbeitsschutz und Arbeitsmedizin, Prof. Ulrich Kelber, Bundesbeauftragter für Datenschutz und Informationsfreiheit, Prof. Marita Körner, Universität Hamburg, Thomas Koczelnik, Konzernbetriebsrat Deutsche Post DHL Group, Dr. Ariane Reinhart, Continental AG, Prof. Anne Richert, Frankfurt University of Applied Sciences, Prof. Rüdiger Krause, Universität Göttingen, Benedikt Rüdesheim, Rechtsanwalt, Prof. Sabine Sachweh, Fachhochschule Dortmund, Prof. Judith Simon, Universität Hamburg, Prof. Jürgen Taeger, Universität Oldenburg, Prof. Georg Thüsing, Universität Bonn, Tim Wybitul, Rechtsanwalt, Prof. Peter Wedde, Frankfurt University of Applied Sciences.

Grundlage für die Arbeit des Gremiums werden umfassende Anhörungen von Verbänden und Gewerkschaften sowie Unternehmen, Datenschutzbeauftragten, Betriebsräten und Beschäftigten bilden, die konkrete Handlungsbedarfe aus ihrer Perspektive formulieren.

Mit dem Beirat zum Beschäftigtendatenschutz setzt das BMAS den im Koalitionsvertrag verankerten Prüfauftrag zur Einführung eines eigenständigen Gesetzes zum Beschäftigtendatenschutz um. Die Einrichtung des Beirats schließt an die Arbeit der von der Bundesregierung eingesetzten Datenethikkommission an, die im Herbst 2019 ihr Gutachten vorgelegt hat. Darin empfahl sie der Bundesregierung, gemeinsam mit den Sozialpartnern gesetzliche Konkretisierungen des Beschäftigtendatenschutzes zu entwickeln (Bundesarbeitsministerium, PE 16.06.2020: Beirat zum Beschäftigtendatenschutz nimmt seine Arbeit auf).

**Bundesweit**

## Sicherheitslücken bei HPI-Schul-Cloud

Journalistenrecherchen des RBB zeigten schwere Sicherheitslücken bei der Schul-Cloud des Potsdamer Hasso-Plattner-Instituts (HPI) auf. Die Cloud wird von Schulen in vielen Bundesländern, u.a. in Niedersachsen, Berlin und Brandenburg genutzt. Von beliebigen Internet-Rechnern war es möglich, ohne Insiderwissen das sogenannte „Ticketsystem“ der Cloud aufzurufen. Hier können sich Nutzer der Cloud, ob Lehrer oder Schüler, an die Administratoren wenden, wenn es Probleme gibt. Abrufbar waren die Vor- und Nachnamen von Schülern, auch Email-Adressen von Anwendern und Schulen. Die HPI-Schul-Cloud wirbt besonders mit der „Einhaltung der geltenden Datenschutzbestimmungen“.

HPI wurde am 14.05.2020 über die Angriffsmöglichkeiten informiert und um Stellungnahme gebeten. Anstatt zu antworten, ging das HPI am 18.05.2020 an die Öffentlichkeit und vermeldete einen illegalen Hackerangriff. Es habe die Datenschutz-Lücke sofort geschlossen, so HPI-Direktor Christoph Meinel. Erst nach weiteren vier Tagen bestätigte HPI gegenüber den recherchierenden Journalisten, „dass in den Tickets tatsächlich personenbezogene Informationen enthalten waren. Insofern bestand in den von Ihnen aufgezeigten Einzelfällen tatsächlich vorübergehend die Möglichkeit eines unbefugten Zugriffs auf personenbezogene Tickets durch Dritte“. Das HPI bedauere diese Zugriffsmöglichkeit, die man sofort beendet habe.

Die Schul-Cloud ist ein politisches Renommierprojekt. Nach HPI-Angaben findet es in etwa 300 Schulen als Pilotprojekt Anwendung und wirbt damit: „Wir sind speziell auf Schulen ausgerichtet

und decken die datenschutzrechtlichen Anforderungen von Schulen ab!"

Mit Hilfe von IT-Fachleuten wurden weitere Sicherheitslücken entdeckt. Mit einer Einmal-Mail-Adresse gelang es, sich einen Account in der Schul-Cloud zuzulegen. Damit konnten die Namen der beteiligten Schulen in einem Bundesland aufgerufen werden und mit wenigen weiteren Klicks die Namen angemeldeter Schüler und Schülerinnen. Über einen anderen Pfad war es mühelos möglich, an eine Liste mit mehreren Tausend Schülernamen zu kommen, die sich am Schul-Cloud-Chat beteiligen.

Das HPI bestätigte, dass der „skizzierte Angriff tatsächlich durchgeführt werden" konnte. Man habe aber auch diese Schwachstelle geschlossen und sämtliche betroffenen Datenschutzbehörden und Schulen informiert. Man habe „Strafanzeige gegen Unbekannt" wegen eines Zugriffs auf Daten einer Schule im Saarland erstattet mit dem Vorwurf des Ausspähens von Daten und der Datenhehlerei. Das HPI argumentierte, der Zugriff auf Personendaten sei nur über öffentlich nicht zugängliche Registrierungslinks möglich gewesen. Einbezogene Experten verwunderte diese Aussage, da die Daten offen und ungeschützt verfügbar waren; der Registrierungslink war öffentlich via Google abrufbar. Das HPI beharrte auch nach einer Nachfrage darauf, dass die Registrierungs-Links vom HPI ausschließlich den Schulen für den internen Gebrauch überlassen worden seien, eine sonstige Nutzung durch Dritte somit rechtswidrig.

Der Jurist und frühere Datenschutzbeauftragte von Schleswig-Holstein, Thilo Weichert, bewertete diese HPI-Argumentation als „unverschämt". Wenn Daten nicht ausreichend geschützt würden, könne man gar nicht von einem rechtswidrigen Zugriff sprechen: „Die schlechte Absicherung des Systems" bei der HPI-Schul-Cloud sei unzulässig. Er zeigte sich sehr verblüfft, wie einfach es möglich war, von jedem Netzrechner aus in das System einzudringen und die „Daten der Schulen einschließlich der Angaben zu den Schülerinnen und Schülern auszuspionieren".

Der Direktor des HPI Christoph Meinel wies diese Kritik zurück: „Systemische Sicherheitslücken sehen wir nicht, uns ist jedoch bewusst, dass es nahezu unmöglich ist, eine komplexe Software beweisbar ohne Sicherheitslücken zu implementieren und zu betreiben. Unser Informationssicherheitsmanagementsystem ist noch jung und insbesondere in einem so rapide wachsenden, agilen Team können menschliche Fehler nicht ausgeschlossen werden."

Das Bundesministerium für Bildung und Forschung (BMBF) fördert das HPI-Projekt seit 2016 mit gut sieben Millionen Euro bis 2021, um am Ende für deutschlandweit 44.000 Schulen eine IT-Lern-Infrastruktur anbieten zu können. Das Ministerium teilte mit, man habe sich „nach Bekanntwerden der aktuellen Sicherheitsvorfälle" vom HPI „über die Vorfälle und Maßnahmen informieren lassen". Eine aktuelle Ankündigung einer weiteren Zuwendung in Höhe eines zweistelligen Millionenbetrags für die Entwicklung der HPI-Cloud von Bildungsministerin Anja Karliczek (CDU) alarmierte die grüne Bundestagsabgeordnete Ekin Deligöz: Offenkundig habe das Forschungsministerium „nicht richtig hingeschaut und Zuwendungen in Millionenhöhe bewilligt, ohne den Datenschutz hinreichend geprüft zu haben."

Der Sprecher der Landesdatenschutzbehörde von Brandenburg Sven Müller teilte mit, es könnten sich „im Quelltext dieses umfangreichen Projekts weitere Fehler befinden, die zu anderen Sicherheitslücken führen können." Das HPI unternehme daher umfangreiche Tests; die Aufklärung dauere an. Erst danach werde man über „aufsichtsrechtliche Maßnahmen unserer Behörde gegenüber dem HPI" entscheiden. Padeluun von der Bürgerrechtsorganisation „Digitalcourage e.V." zeigte sich über die Rechercheergebnisse sehr besorgt: „Dieses System muss durch die Aufsichtsbehörden abgeschaltet werden, bevor die sensiblen Daten von Schülerinnen und Schülern in dunkle Kanäle umgeleitet werden" (Adamek/Opalka, HPI-Schul-Cloud wies schwere Sicherheitslücken auf, www.rbb24.de 20.05.2020).

**Bundesweit**

## Apple-Maps-Kamerawagen unterwegs

Apple schickte Kamerawagen von Juni bis September 2020 durch Deutschland, um „Vermessungsfahrten" und „Bilderfassungen" durchzuführen. Nur Autos sollen in den dreizehn Bundesländern sowie Berlin, Bremen und Hamburg unterwegs sein; Bilderfassungen mit „tragbaren Systemen", etwa in Fußgängerzonen, sind nach Apple-Angaben nicht vorgesehen. Wie viele Kamerawagen dafür eingesetzt werden und wie umfassend das deutsche Straßennetz abgebildet werden soll, blieb zunächst unklar. Apple war 2019 bereits mit gut 80 Autos in Deutschland ebenso wie in anderen europäischen Ländern unterwegs. Neben Kameras dürften die Fahrzeuge wieder mit verschiedenen Sensoren, darunter Light-Detection-and-Ranging-Sensoren (Lidar) ausgerüstet sein, die die Umgebung dreidimensional erfassen können.

Die Vermessungsfahrten bilden die Grundlage für Apples großangelegte Renovierung des hauseigenen Kartendienstes. Seit Anfang 2020 zeigt Apple in den USA eine neue Kartenversion, die im Laufe des Jahres auch nach Europa kommen soll. Ob zu den abgedeckten Ländern auch Deutschland gehört, ist offen. Teil der neuen Version von Apple Maps respektive Apples Karten-App in iOS 13 ist die Funktion „Umsehen" (Look Around) – ein Pendant zu Googles Streetview, mit dem man Städte praktisch auf Augenhöhe „durchfahren" kann. Derzeit sind so einige wenige US-Städte abgedeckt.

2019 hatten Datenschutzbehörden darauf hingewiesen, dass bei der Einführung einer solchen Funktion in Deutschland eine „leicht zugängliche Widerspruchsmöglichkeit" angeboten werden muss. Apple verspricht, dass Gesichter und Nummernschilder auf den Aufnahmen automatisch unkenntlich gemacht werden. Wer die Verpixelung seines Hauses beantragen will, kann sich per E-Mail an den Konzern wenden (Becker, Apple Maps: Kamerawagen in ganz Deutschland unterwegs, www.heise.de 09.06.2020, Kurzlink: https://heise.de/-4779084).

**Bundesweit**

## Datenschutzbehörden gegen Glücksspielstaatsvertrag

Die Landesdatenschutzbeauftragten meinen, dass der im März 2020 be-

schlossene Glücksspielstaatsvertrag in mehrfacher Hinsicht das Grundrecht auf Datenschutz verletzt. Dieser sieht ab Juli 2021 die Schaffung einer Behörde mit Sitz in Sachsen-Anhalt vor, die Glücksspiel im Internet, also virtuelle Automaten, Pokertische oder Blackjack-Runden, überwacht. Auch für die Online-Auftritte der im Fußball omnipräsenten Sportwettangebote soll die Aufsichtsbehörde bundesweit zuständig sein. Damit wollen die Bundesländer erstmals Online-Angebote erlauben; es soll Schluss sein mit milliardenschweren unregulierten Grau- und Schwarzmärkten, auf denen sich Sportwett- und Casinoanbieter bislang bewegen.

Nach Ansicht der Landesdatenschutzbeauftragten sind die Länder dabei aber über das Ziel hinausgeschossen. In einem Schreiben an die Staatskanzlei des Landes NRW bemängelt der sächsische Datenschutzbeauftragte Andreas Schurig als Vorsitzender der Datenschutzkonferenz erhebliche Probleme, die der neue Glücksspielstaatsvertrag mit sich bringe. Unter anderem rät er dringend von der Einrichtung zentraler Dateien ab, mit denen die neue Glücksspielbehörde das Online-Spiel überwachen will. Nordrhein-Westfalen war federführend für die CDU-geführten Länder bei den Beratungen zum Glücksspielstaatsvertrag.

Das Regelwerk sieht als Teil der Suchtprävention vor, dass Spieler anbieterübergreifend nicht mehr als 1.000 Euro pro Monat einzahlen dürfen. Das soll die neue Magdeburger Behörde permanent in einer zentralen Datei überwachen. Spieler würden darin unter anderem mit Namen, Geburtsdatum, Anschrift und ihren Einzahlungen gespeichert, was die Online-Aktivitäten eines Spielers staatlicherseits vollständig nachvollziehbar mache, schreibt Schurig: „Glücksspiel findet nicht mehr statt, ohne dass der Staat Kenntnis vom Spieler und seinen konkreten Spieleinsätzen erlangt.“ Er kritisiert außerdem, dass die Daten ein Jahr gespeichert bleiben sollen. Eine solche Datei sollte nicht geschaffen werden.

Zudem bemängeln die Datenschutzbeauftragten zwei weitere Dateien. Die neue Behörde soll zentral überwachen, dass Spieler immer nur bei einem Anbieter gleichzeitig spielen - womit gespeichert würde, wann ein Spieler aktiv gewesen ist. Ein Algorithmus soll suchtgefährdete und süchtige Spieler identifizieren, was im Gesetz aber unklar formuliert und nach der Datenschutz-Grundverordnung wohl rechtswidrig sei.

Anfang 2020 hatte der Ex-Bundesdatenschutzbeauftragte Peter Schaar vor einer „Totalüberwachung von Spielern“ gewarnt. Im März hatten sich die Ministerpräsidenten der Länder nach jahrelangen Verhandlungen auf die Neufassung des Glücksspielstaatsvertrags geeinigt. Um in Zukunft effektiver gegen illegale Angebote vorzugehen, sind Netzsperren vorgesehen, zu denen die Regulierung Netzbetreiber verpflichten könnte. Bislang beschränkt sich das Vorgehen auf die Unterbindung von Zahlungsströmen. Der von den Ministerpräsidenten beschlossene Staatsvertrag wird noch von der EU-Kommission geprüft. Die 16 Länderparlamente sollen den Vertrag im Herbst 2020 ratifizieren (Willmroth, Datenschützer kritisieren Glückspielregeln, SZ 12.06.2020, 22).

### Bund

## Regierungskoalition einigt sich auf Lobbyregister

Nach langem Widerstand aus den Unionsparteien hat sich die große Koalition von CDU/CSU und SPD am 03.07.2020 auf ein verbindliches Lobbyregister für den Bundestag verständigt. Die Affäre um den CDU-Abgeordneten Philipp Amthor hatte Bewegung in die Gespräche gebracht. Amthor hatte sich beim Wirtschaftsministerium für das US-amerikanische IT-Unternehmen Augustus Intelligence eingesetzt. Für die Union teilten in Berlin Fraktionsvize Thorsten Frei und der zuständige Berichterstatter Patrick Schnieder mit, dass schärfere Transparenzregeln für Interessensvertreter gegenüber dem Bundestag und seinen Mitgliedern gelten werden.

Verstöße gegen das Register sollen sanktioniert werden können. SPD-Fraktionsvize Dirk Wiese und sein Kollege Matthias Bartke kündigten eine schnelle Verabschiedung an: „Wir haben eine Lösung gefunden, die deutlich mehr Transparenz herstellt, ohne dass der wichtige Kontakt zu Abgeordneten erschwert wird“. Auch für den CDU-Politiker Schnieder ist die Einigung mit dem Koalitionspartner SPD ein echter Erfolg: „Vor allem der verpflichtende Charakter des Lobbyregisters ist wichtig. So haben wir uns insbesondere darauf verständigt, dass Verstöße gegen die Registrierungspflicht durch die Einführung eines neuen Ordnungswidrigkeitentatbestandes zukünftig bußgeldbewehrt sein werden.“

Linken-Chef Bernd Riexinger begrüßte die Einigung der Koalition als einen überfälligen Schritt, um den Einfluss der Wirtschaft auf die Gesetzgebung zurückzudrängen. Allerdings seien weitere Schritte nötig, um die Demokratie vor dem Einfluss finanzstarker Lobbygruppen zu schützen: „Es muss ein Beschäftigungsverbot für Lobbyistinnen und Lobbyisten in Bundesministerien und von Abgeordneten bei Unternehmen und Lobbyorganisationen folgen. Wer Gesetze schreibt, darf nicht gleichzeitig von ihnen profitieren. Die Nebenverdienste von Abgeordneten, inklusive aller geldwerten Leistungen, müssen auf Euro und Cent veröffentlicht werden.“ Die Oppositionsparteien FDP, Linke und Grüne haben bereits Anträge zu einem solchen Register vorgelegt.

Transparency Deutschland begrüßte die Einigung ebenfalls. Endlich habe sich die Koalition entschlossen, etwas gegen intransparenten Lobbyismus und den damit verbundenen Ansehensverlust der Politik zu unternehmen: „Allerdings erwarten wir eine umfassende gesetzliche Regelung, die auch für die Bundesregierung gilt.“ 80% der Gesetze würden von der Bundesregierung initiiert, und wichtige Gespräche würden in den Ministerien geführt, wie der Fall Amthor zeige (Union und SPD einigen sich auf verbindliches Lobbyregister, www.heise.de 03.07.2020).

### Bund

## Kartellamt geht gegen Smart-TV-Hersteller vor

Das Bundeskartellamt hat schwere Mängel beim Datenschutz und der IT-Sicherheit bei vernetzten Fernsehgeräten ausgemacht und fordert von den Herstellern umfangreiche Nachbesserungen. Es verweist zudem auf weitere

Probleme wie „die Rechtmäßigkeit von Werbeeinblendungen im TV-Portal". Die in Deutschland aktiven Smart-TV-Hersteller zeigten fast durchgehend schwerwiegende Transparenzmängel rund um die Privatsphäre der Verbraucher. Damit verstießen sie massiv gegen die Datenschutz-Grundverordnung.

Die Geräte können laut der „Sektoruntersuchung Smart-TVs" vielfältig personenbezogene elektronische Spuren erheben. So könnten das generelle Fernsehverhalten einer Person, ihre App-Nutzung, ihr Surf- und Klickverhalten oder auch biometrische Daten wie Stimme oder Cursorbewegungen sowie die im Einzelnen über den Fernseher abgespielten Inhalte erfasst und ausgewertet werden. Dass die Hersteller solch intime Nutzungsdaten sammeln und etwa für personalisierte Werbung verwenden, könne der Verbraucher meist nur verhindern, indem er Einstellungen an seinem Fernsehgerät ändert und sich durch zahlreiche Menüs hangelt. Sich über die Datenschutzbestimmungen bereits vor dem Kauf zu informieren, sei oft nicht oder nur mit großem Aufwand möglich. Bei der Ersteinrichtung fügten sich die meisten Kunden zudem den angezeigten Bedingungen, da sie dazu keine Alternative sähen.

Für die Käufer sei meist nicht nachvollziehbar, dass die Datenschutzbestimmungen „für eine Vielzahl von Diensten und Nutzungsprozessen gelten sollen". Die Verbraucher erführen nicht zuverlässig, welche personenbezogenen Daten verarbeitet, für wie lange gespeichert und an Dritte übermittelt werden. Etliche Hersteller gewährleisten zudem nicht, dass der Standard der Geräte für IT-Sicherheit auch in den Jahren nach dem Kauf durch Software-Aktualisierungen aufrechterhalten wird; dazu mache kein Unternehmen verbindliche Angaben. Für die Verbraucher sei diese Information aber unerlässlich, „um einschätzen zu können, wie lange sie das Gerät uneingeschränkt gefahrlos verwenden können".

Das Bundeskartellamt fordert, dass Nutzer besser und zielgerichteter „über die Möglichkeit zur extensiven Datensammlung und -verarbeitung" durch alle Geräte im Internet der Dinge aufgeklärt werden. Die Unternehmen sollten notwendige Informationen klarer und einfacher vermitteln müssen. Anwendern sollte es leichter gemacht werden, Datenschutzstandards schon vor dem Kauf etwa durch eingängige Bildsymbole zu berücksichtigen. Nötig sei zudem ein „klarer gesetzlich geregelter Anspruch des Verbrauchers auch gegenüber dem Hersteller auf Software-Updates". Der Gesetzgeber solle auch Haftungsfragen beim Zusammenspiel der verschiedenen Akteure im Bereich des „Internet of Things" (IoT) klären. Die Kontrolleure hatten die Untersuchung im Dezember 2017 auf Basis neu erhaltener verbraucherrechtlicher Kompetenzen eingeleitet. Die Ermittlungen betrafen rund 20 Anbieter, die in Deutschland internetfähige Fernsehgeräte unter eigenen Marken absetzen (Krempl, Bundeskartellamt: Smart-TV-Hersteller verstoßen massiv gegen die DSGVO, www.heise.de 02.07.2020, Kurzlink: https://heise.de/-4801949).

### Baden-Württemberg

## Millionenbußgeldbescheid gegen AOK wegen Werbenutzung

Wegen eines Verstoßes gegen die Datenschutz-Grundverordnung (DSGVO) hat die AOK Baden-Württemberg vom Landesbeauftragen für den Datenschutz in Stuttgart (LfDI BaWü) ein Bußgeld in Höhe von 1,24 Mio. € auferlegt bekommen. Sie habe 2015 bis 2019 Gewinnspiele veranstaltet und dabei personenbezogene Daten der Teilnehmer gesammelt, darunter deren Kontaktdaten und Krankenkassenzugehörigkeit, um die Daten der Gewinnspielteilnehmer für Werbezwecke zu nutzen. Gemäß einer Mitteilung des LfDI BaWü wollte die AOK mit internen Richtlinien und Datenschutzschulungen sicherstellen, dass nur Daten jener Gewinnspielteilnehmer zu Werbezwecken verwendet werden, die zuvor eingewilligt hatten. Dennoch seien die personenbezogenen Daten von mehr als 500 Gewinnspielteilnehmern ohne deren Einwilligung zu Werbezwecken verwendet worden.

Nachdem ihr der Vorwurf bekannt wurde, habe die AOK sofort den Vertrieb eingestellt, um sämtliche Abläufe gründlich zu prüfen, eine Task Force eingesetzt, die Einwilligungserklärungen angepasst und interne Prozesse und Kontrollstrukturen geändert. Bei der Bemessung der Geldbuße sei neben der Größe und Bedeutung der AOK Baden-Württemberg berücksichtigt worden, dass sie als eine gesetzliche Krankenversicherung wichtiger Bestandteil des Gesundheitssystems sei: „Weil Bußgelder nach der DSGVO nicht nur wirksam und abschreckend, sondern auch verhältnismäßig sein müssen, war bei der Bestimmung der Bußgeldhöhe sicherzustellen, dass die Erfüllung dieser gesetzlichen Aufgabe nicht gefährdet wird." Die seit gut zwei Jahren geltende Regelung gibt den Aufsichtsbehörden die Befugnis, bei Verstößen Geldstrafen von bis zu vier Prozent der weltweiten Einnahmen oder 20 Mio. € durchzusetzen. Die bisher höchste Strafe wurde Google mit 50 Mio. € in Frankreich auferlegt (Wilkens, DSGVO-Verstoß: AOK Baden-Württemberg soll 1,2 Millionen Euro geldbüßen, www.heise.de 30.06.2020, Kurzlink: https://heise.de/-4799680).

### Bundesweit

## Polizeiliche Gesichtserkennung nimmt massiv zu

Das umstrittene Ermittlungsverfahren der biometrischen Gesichtserkennung wird zunehmend zum Standardinstrument von Strafverfolgern in Deutschland. Deutsche Polizeibehörden haben im BKA-Gesichtserkennungssystem GES 2019 fast 54.000 Recherchen durchgeführt, während es 2017 noch 27.000 waren. Beim Bundeskriminalamt (BKA), das in diesem Bereich in Deutschland als Zentralstelle fungiert, wachsen die Datenbanken für Porträts an und werden immer häufiger genutzt. Aus einer Antwort der Bundesregierung auf eine Anfrage der Linksfraktion im Bundestag geht hervor, dass 2017 Ermittler von Bund und Ländern im zentralen BKA-Gesichtserkennungssystem GES rund 27.000 Recherchen durchgeführt haben. Im ersten Halbjahr 2018 waren es bereits 20.749, wobei 320 Personen identifiziert werden konnten. 2019 nahmen die Beamten nun insgesamt 53.971 Abfragen in der Datenbank vor, mit deren Hilfe sie insgesamt 2.123 Personen identifizier-

ten. Die Zahl der Recherchen stieg damit gegenüber 2017 um fast 60%.

Das BKA selbst führte mit 27.523 Zugriffen fast exakt die Hälfte der GES-Recherchen in 2019 durch, konnte mit 187 ausgemachten Personen die Technik aber nicht sehr gewinnbringend nutzen. Auf das Konto der Landeskriminalämter gehen 21.251 Abfragen, mit denen diese immerhin 1.488 Betroffene identifizieren konnten. Inwieweit sich in der Statistik noch die Folgen der vielkritisierten biometrischen Fahndung der Polizei Hamburg nach Randalierern beim G20-Gipfel 2017 in der Hansestadt niederschlagen (DANA 4/2018, 199 f.), geht aus der Antwort nicht hervor.

Die Bundespolizei führte 5.197 Recherchen im GES durch und landete dabei 448 positive Treffer. Ein Plan von Bundesinnenminister Horst Seehofer (CSU), wonach die einstigen Grenzschützer an Bahnhöfen und Flughäfen eine „intelligente Videoüberwachung" mit Mustererkennung verwenden und dabei gegebenenfalls auch biometrische Daten abgleichen dürfen sollen, wurde auf Eis gelegt (vgl. DANA 1/2020, 38). Nach Ansicht der Regierung stellt das bestehende Bundespolizeigesetz zumindest für den Einsatz der auch auf EU-Ebene diskutierten Systeme zur „Live-Gesichtserkennung" keine hinreichende rechtliche Basis dar. Dafür „wäre vielmehr eine eigenständige gesetzliche Ermächtigungsgrundlage erforderlich", welche die einschlägigen Voraussetzungen „unter Beachtung verfassungsrechtlicher Anforderungen hinreichend bestimmt".

Das BKA führt zudem laut der Antwort im Bereich Biometriesystemen eine Amtsdatei „ST-Libi-Z". Sie diene der Polizeibehörde im Kampf gegen politisch motivierte Kriminalität „zur Speicherung der im Rahmen ihrer Aufgabenwahrnehmung anfallenden digitalen Lichtbilder und der Identifizierung von unbekannten polizeilich relevanten Personen mittels automatisierter Lichtbildvergleiche". Mit Stand vom 19.03.2020 umfasste diese Datenbank demnach insgesamt 3.519 Fotos zu 2.950 Personen aus dem Bereich „Politisch motivierte Kriminalität – Religiöse Ideologie".

Der Bestand an recherchefähigen Porträtbildern im zentralen polizeilichen Informationsverbund Inpol stieg gemäß den Angaben des BMI von 5,50 Mio. Lichtbildern Anfang 2019 auf rund 5,81 Mio. am 02.01.2020. Der „Netto-Aufwuchs" habe demnach rund 310.000 Aufnahmen innerhalb von zwölf Monaten betragen, was einem Plus von fast 5,5% entspricht: „Eine detaillierte Auswertung zur Anzahl sowie zu den Gründen der hinzugekommenen und gelöschten Lichtbilder ist aufgrund der Corona-Lage zurzeit nicht möglich." Im einschlägigen System Inpol-Z seien Anfang Januar 3.648.613 Personen mit Porträtfotos gespeichert gewesen.

Der europapolitische Sprecher der Linksfraktion, Andrej Hunko, bezeichnete „die abermals stark steigenden Zahlen [als] absolut besorgniserregend". Sie belegten, „dass die Gesichtserkennung durch Behörden unbedingt eingehegt werden muss". Für Abfragen im Inpol-System würden auch Bilder aus der Videoüberwachung im öffentlichen Raum genutzt, was wohl den Zuwachs bei der Bundespolizei erklärte. Eine Reform des Bundespolizeigesetzes, mit der die Gesichtserkennung an Verkehrsknotenpunkten sogar automatisiert erfolgen dürfte, „müssen wir deshalb unbedingt verhindern" (Krempl; Überwachung: BKA und LKAs weiten Einsatz von Gesichtserkennung deutlich aus, www.heise.de 30.04.2020, Kurzlink: https://heise.de/-47129569).

**Bayern**

## Corona-Gästelisten für Polizeiermittlungen genutzt

Die Bayerische Polizei hat für Ermittlungen auf die Daten aus Wirtshäusern oder Biergärten zugegriffen, die im Rahmen der Bekämpfung der Corona-Pandemie angelegt wurden. Dies ist in mindestens zehn Fällen passiert. Die Gästedaten, die beim Besuch eines Lokals angegeben werden müssen, sind eigentlich zur Verfolgung möglicher Infektionsketten gedacht. Der Innenminister des Freistaates Joachim Herrmann (CSU) rechtfertigte dies: „Der Bürger erwartet zu Recht, dass die Polizei im Rahmen der Rechtsordnung alles zu seinem Schutz unternimmt und nicht unter dem Deckmäntelchen eines falsch verstandenen Datenschutzes die Hände in den Schoß legt."

Die Polizeipräsidien betonten, dass sie nur bei entsprechend schwerwiegenden Delikten auf die Daten zugreifen würden. In Ober- und Mittelfranken nutzten Polizisten die Daten jeweils zur Aufklärung versuchter Tötungsdelikte, in Schwaben zum Beispiel bei der Vermisstensuche nach einem Wanderer; das Landeskriminalamt nutzte außerdem Daten von Gästen nach einem mutmaßlichen Rauschgiftdelikt in einem Wirtshaus. Dass sie mit den Listen auf sensible Daten zugreifen, ist den Beamten, so die Auskunft der Präsidien, bei ihren Abwägungen klar. Auch wenn die Daten grundsätzlich nur für den eigentlichen Zweck genutzt werden dürften, sei für die Aufklärung von Delikten laut Strafprozessordnung eine „Zweckänderung" möglich.

Teile der Landtagsopposition hatten sich nach Bekanntwerden der Fälle empört gezeigt. Grünen-Fraktionschefin Katharina Schulze sagte, sie könne die Irritation der Menschen über diesen Vertrauensbruch absolut nachvollziehen. „Meine große Sorge ist, dass Leute sich vielleicht denken: ‚Dann schreibe ich vielleicht einen falschen Namen auf die Liste, weil wer weiß, an wen diese Daten überhaupt kommen'". Dies habe ernsthafte Konsequenzen für die Pandemiebekämpfung. Martin Hagen, FDP-Fraktionsvorsitzender, meinte: „Das Beteuern der Polizei, die Daten nur bei besonders schwerwiegenden Delikten zu nutzen, reicht nicht aus. Gästedaten müssen tabu sein. Das muss gesetzlich klargestellt werden."

Herrmann hielt dem entgegen, bei der Zeugensuche nach einem Mordversuch sollte man nach Auffassung von FDP und Grünen wohl „den Täter lieber laufen lassen, anstatt die Gästedaten beizuziehen?" Das sei „völlig absurd". In dem Fall in Schwaben sei es um Leben und Tod gegangen. „Einen vermissten Wanderer würden Herr Hagen und Frau Schulze wohl auch lieber seinem Schicksal überlassen." Martin Hagen konterte am Wochenende über Social Media: „Sehr geehrter Herr Innenminister, (...) wenn künftig nur noch Max Mustermann und Micky Maus im Restaurant einchecken, wird die Nachverfolgung von Infektionsketten unmöglich." Und Katharina Schulze: „Unsachliche Polemik bringt uns nicht weiter. Mir geht es

um eine bundeseinheitliche Regelung, und dazu braucht es ein Begleitgesetz. Damit wird Klarheit für Wirtsleute und Gäste geschaffen, dass die erhobenen Daten nicht willkürlich, sondern nur zu explizit definierten Ermittlungszwecken verwendet werden dürfen." Das Vertrauen in die Akzeptanz für die Corona-Verordnungen zu stärken „sollte auch im Interesse des zuständigen Innenministers sein". Der Landesdatenschutzbeauftragte Thomas Petri mahnte ebenso eine bundesweit einheitliche Lösung an, auch wenn die Zweckentfremdung der Listen, „isoliert betrachtet", rechtmäßig sei (Osel, „Deckmäntelchen Datenschutz", SZ 20.07.2020, 28).

**Berlin**

## Schlagabtausch wegen Teams und Skype

Die Berliner Datenschutzbeauftrage Maja Smoltczyk hat vor der Nutzung der Videokonferenzsysteme Skype und Teams, die von Microsoft angeboten werden, gewarnt. Der Chefjurist von Microsoft Deutschland hat sich daraufhin an Smoltczyk gewendet und diese aufgefordert, „unrichtige Aussagen (...) zu entfernen und zurückzunehmen". Es geht um die grundsätzliche Frage, ob Behörden, Schulen und andere Unternehmen die Software von Microsoft legal einsetzen können. Der Streit entzündete sich an zwei Dokumenten, die Smoltczyk im April 2020 auf ihrer Webseite veröffentlichte. Beide enthalten Empfehlungen zur „Durchführung von Videokonferenzen während der Kontaktbeschränkungen". Darin rät Smoltczyk Unternehmen, Behörden und anderen öffentlichen Einrichtungen davon ab, die Microsoft-Dienste Teams und Skype zu verwenden.

Am Morgen des 18.05.2020 waren beide Dokumente noch abrufbar; im Laufe des Vormittags wurden sie ohne weiteren Hinweis entfernt. Eine Sprecherin der Datenschutzbeauftragten erklärte, die Behörde habe ein Schreiben von Microsoft erhalten, dessen Inhalt man prüfe. Microsoft betonte, dass es sich nicht um eine juristische Abmahnung handle, wie manche Medien berichtet hatten; der Brief entspräche inhaltlich einer Pressemitteilung, die Microsoft bereits Anfang Mai veröffentlicht hatte. Darin hieß es, dass Teams und Skype datenschutzkonform seien. Smoltczyks Einschätzung enthalte „missverständliche Aussagen und legt zum Teil unzutreffende datenschutzrechtliche Wertungen zugrunde". Eine Sprecherin sagte, Microsoft habe um Richtigstellung gebeten und werde sich deswegen mit der Behörde austauschen.

In den Ausführungen der Datenschutzbehörde von Berlin war nicht völlig klar, was Microsoft vorgeworfen wird: „Die oben beschriebenen Risiken verbleiben jedoch ... Prominentes Beispiel sind die Dienstleistungen [von Microsoft und Skype]". Im Abschnitt „Risiken" wird gewarnt, „dass bei der Videokonferenz unbefugt mitgehört oder aufgezeichnet und die Inhalte weiter ausgewertet werden" könne. Ob Smoltczyk alle genannten Risiken auch auf Microsoft bezieht, oder nur die Vereinbarkeit mit der europäischen Datenschutz-Grundverordnung (DSGVO) anzweifelt, blieb offen.

Nach Überprüfung der Dokumente erklärte die Datenschutzbehörde, es habe sich kein inhaltlicher Änderungsbedarf der Empfehlungen ergeben, die wieder ins Netz gestellt wurden. „Es wurden nur einige geringfügige Konkretisierungen an den Texten vorgenommen." In Bezug auf Zoom geht aus dem Dokument indirekt hervor, woran sich die Datenschützer unter anderem stören. Sie verweisen darauf, dass sich bei einem Rückgriff auf die internationale Datenschutzvereinbarung „Privacy Shield" die Zertifizierung auch auf Personaldaten erstrecken müsse. Bei Zoom fehlt ein solches HR-Zertifikat.

Warum die Microsoft-Dienste Teams und Skype den Voraussetzungen nicht entsprechen, wird in dem Dokument nicht im Detail erläutert. Allerdings kündigt die Behörde an, „in Kürze eine ausführlichere Übersicht mit detaillierteren Angaben zu verschiedenen gängigen Anbietern von Videokonferenz-Diensten zu erstellen".

Die Stiftung Warentest hatte kurz zuvor Videokonferenz-Systeme getestet und dabei die Datenschutzerklärungen untersucht. Diese ließen, so das Ergebnis, bei Microsoft „keine ernsthafte Befassung mit der DSGVO erkennen". Dennoch landen Teams und Skype auf den Rängen 1 und 2, die Datensicherheit wird jeweils mit gut bewertet. Der Journalist und Datenschutzexperte Matthias Eberl, der auf seiner Webseite eine Analyse veröffentlichte, erklärte dazu, dass die schlampige Datenschutzerklärung völlig ausreiche: „Teams lässt sich nicht rechtskonform einsetzen, das ist keine Frage der Meinung." Gemäß der Untersuchung übertragen sowohl die Gratis-Version von Teams als auch die Variante für Bildungseinrichtungen Nutzerdaten an die Werbenetzwerke von Adobe und Google, obwohl Microsoft eine Verwendung von Kundendaten für Werbung ausschließt.

Die Nachfrage nach Videokonferenz-Software ist seit Beginn der Corona-Krise stark gestiegen. Davon profitiert bislang hauptsächlich das vergleichsweise kleine Zoom, doch große Tech-Unternehmen wie Facebook, Google und Microsoft haben schnell reagiert und ihre eigenen Dienste nachgerüstet. Jeder will ein Stück vom Video-Kuchen haben. Da kam die Warnung der Landesdatenschutzbeauftragten zur Unzeit. Im Hintergrund dieser Warnung steht die grundsätzliche Frage, welche kommerzielle Software öffentliche Stellen wie Behörden, Schulen und Universitäten einsetzen sollen und dürfen. 2019 hatte etwa der hessische Beauftragte für Datenschutz Schulen zwischenzeitlich verboten, das Office-Paket Microsoft 365 zu nutzen. In Baden-Württemberg warnte der zuständige Datenschützer Stefan Brink vor Zoom und Microsoft und riet zu datenschutzfreundlichen Open-Source-Lösungen. Von der Debatte ist nicht nur Microsoft betroffen. So meinte der Bundesbeauftragte für Datenschutz Ulrich Kelber, „dass der Einsatz von Whatsapp für eine Bundesbehörde ausgeschlossen ist". Der Messenger erfasst zwar keine Inhalte, sammelt aber Verbindungsdaten: Wer schreibt wann und wie oft mit wem? Kelber vermutet, dass diese Daten beim Mutterkonzern Facebook landen. Whatsapp sagt, man gebe keine „Benutzer-Metadaten weiter, um Facebook-Profile zu erstellen oder Facebook-Produkte oder -Werbung anderweitig zu verbessern". Dieses sehr spezifische Dementi lässt allerdings weitere Nutzungsmöglichkeiten offen. Es bedeutet nicht, dass gar keine Daten

an Facebook übermittelt werden (Hurtz, Microsoft schickt bösen Brief nach Berlin, www.sueddeutsche.de 18.05.2020; Teams & Co: Berliner Datenschutzbeauftragte legt im Streit mit Microsoft nach, www.heise.de 25.05.2020).

**Bayern**

## Polizei macht fotografierenden Rentner zum potenziellen Sexualtäter

„Es begann harmlos mit den Tücken der modernen Technik und endete für einen 78-jährigen Rentner mit einer erkennungsdienstlichen Behandlung, einer Speichelabgabe für eine DNA-Analyse und der polizeilich gespeicherten Einschätzung, er könne sexuelle Interessen gegenüber Kindern haben." So fasste der bayerische Datenschutzbeauftragte Thomas Petri einen speziellen Fall fehlgeleiteter Polizeiermittlung in seinem Tätigkeitsbericht 2019 zusammen, den er am 25.05.2020 veröffentlichte.

Der Betroffene hatte auf einem belebten Spielplatz mit seinem Handy eine Hüpfburg fotografiert, um das Bild später seinem Enkel zu zeigen. Dabei erregte er offenbar Aufsehen und verstrickte sich anschließend nach Auffassung empörter Eltern in Bezug auf seine Motivlage in Widersprüche. Eine verständigte Streifenbesatzung stellte die Identität des Senioren fest, befragte ihn, stellte sein Mobiltelefon sicher und behandelte ihn im Anschluss daran zur „Abwehr einer konkreten Gefahr" erkennungsdienstlich. Die Beamten führten auch einen Mundhöhlenabstrich durch, um ein DNA-Identifizierungsmuster festzustellen. Gemäß Petri hatte die dabei dem Bürger ausgehändigte Rechtsbelehrung aber auf eine „nicht zutreffende Rechtsgrundlage nach der Strafprozessordnung" verwiesen. Die Polizei verfügt zwar mit dem umstrittenen bayerischen Polizeiaufgabengesetz (PAG) prinzipiell über die weitgehende Befugnis, „insbesondere Finger- und Handflächenabdrucke eines Betroffenen abzunehmen sowie Lichtbilder, Messungen und eine Personenbeschreibung" zu erstellen, aber nur, um eine unbekannte oder zweifelhafte Identität aufzuklären, eine Gefahr für ein bedeutendes Rechtsgut abzuwehren oder Straftaten vorzubeugen, „sofern vom Verdächtigen eine Wiederholungsgefahr ausgeht".

Unter ähnlichen Voraussetzungen darf die Polizei Körperzellen Verdächtiger entnehmen und eine DNA-Analyse durchführen. Petri: „Doch all diese Voraussetzungen trafen auf den hier kontrollierten Rentner nicht zu, insbesondere ging von ihm keine ‚konkrete Gefahr' aus." Ein strafrechtlicher Tatvorwurf sei gar nicht erhoben worden, belastende Vorerkenntnisse hätten nicht vorgelegen. Trotzdem habe der Hobby-Fotograf erst mehrere Stunden nach dem eigentlichen Geschehen nach einer „eindringlichen Ansprache" die Polizeidienststelle wieder verlassen dürfen. Die über den Rentner gewonnenen Informationen gaben die Vollzugsdiener an ein für Sexualdelikte zuständiges Kommissariat weiter. Obwohl die dortigen Ermittler zu dem Schluss kamen, dass keine Hinweise auf eine sexuelle Motivation des Betroffenen vorlagen, zog der Vorfall laut dem Bericht „auf Landes- und sogar Bundesebene zahlreiche Speicherungen zur ‚polizeilichen Gefahrenabwehr' nach sich".

Das sichergestellte Smartphone erhielt der Rentner rund einen Monat später wieder. Mit seinem Einverständnis war darauf eine Videosequenz gelöscht worden, obwohl Petri zufolge „weder rechtlich problematische Daten noch Aufnahmen der besagten Kinder von der Hüpfburg darauf erkennbar waren". Als der betagte Verdächtige später einen Auskunfts- und Löschungsantrag an das Bayerische Landeskriminalamt (LKA) sandte, lehnte dieses das Begehr im Kern ab. Das LKA begründete dies mit der konkreten Gefahr, dass er weitere Hemmschwellen abbauen und aus einer sexuellen Motivation heraus Kinder fotografieren werde. Petri widersprach und stellte klar, „dass eine erste Abklärung des Sachverhalts geboten war, um die Rechte der Kinder auf dem Spielplatz zu wahren". Als sich jedoch frühzeitig herausgestellt hatte, dass der Rentner „keine gezielten Aufnahmen von Kindern gefertigt hatte und auch sonst nichts auf eine sexuelle Motivation" hingedeutet habe, „hätte die Polizei die Situation allerdings sofort neu bewerten müssen". Seinem Appell, „die gespeicherten personenbezogenen Daten unverzüglich zu löschen und die zu dem Betroffenen geführten Akten zu vernichten, wurde schließlich im vollen Umfang Folge geleistet". Petri erinnerte das Polizeipräsidium daran, dass die Ermittler Daten aus polizeilichen Informationssystemen prinzipiell von sich aus spätestens dann löschen müssten, wenn eine Speicherung nicht mehr erforderlich sei. Ein Antrag einer möglicherweise betroffenen Person sei dafür nicht nötig (Krempl, Datenschutz in Bayern: Rentner knipst Hüpfburg, wird als Sexualgefährder erfasst, www.heise.de 25.05.2020, Kurzlink: https://heise.de/-4728207).

**Nordrhein-Westfalen**

## Tönnies-Adressenliste gehen an Pflegeeinrichtungen

Das von Karl-Josef Laumann (CDU) geleitete nordrhein-westfälische Gesundheitsministerium wies per Erlass vom 21.06.2020 die Verteilung einer Tönnies-Liste der Wohnadressen der Beschäftigten bei Pflegeeinrichtungen an. Daraufhin reichten die Gesundheitsbehörden in drei Regierungsbezirken die Liste der vom Corona-Ausbruch betroffenen Beschäftigten am Standort Rheda-Wiedenbrück an Hunderte Pflegeeinrichtungen weiter. Das Gesundheitsministerium bestätigte, dass die Einrichtungen auf dieser Grundlage „schnellstmöglich den erforderlichen Abgleich zu den Wohnorten ihrer Beschäftigten durchführen" sollten, um Überschneidungen schnellstmöglich zurückzumelden.

In den Regierungsbezirken Detmold, Arnsberg und Münster erreichte die Liste mit den Wohnanschriften von über 7.400 Tönnies-Beschäftigten daraufhin zahlreiche Empfänger. Allein in der Stadt Dortmund erhielten 164 Einrichtungen außerhalb von Behörden das Excel-Dokument. Auch der Kreis Warendorf und der Kreis Paderborn bestätigten die dortige Weiterleitung an Einrichtungen. In dem Dokument sind zwar keine Namen enthalten, es lässt aber Rückschlüsse auf Beschäftigte zu.

Der Datenschutzbeauftragte des Landes NRW prüft anlässlich mehrerer Beratungsanfragen den Sachverhalt. Eine

abschließende rechtliche Bewertung liegt noch nicht vor. Das Gesundheitsministerium gibt an, dass es die Weiterleitung der Listen vom Infektionsschutzgesetz und dem Wohn- und Teilhabegesetz gedeckt sehe. Die Datenschutz-Grundverordnung stehe der Maßnahme nicht im Wege. Es sei besonderer Eilbedarf gegeben, um Bewohner der Einrichtungen vor der Corona-Pandemie zu schützen.

Datenschutzinitiativen üben hingegen scharfe Kritik am Vorgehen. Thilo Weichert von der Deutschen Vereinigung für Datenschutz erklärte: „Die Weitergabe der Listen ist eindeutig unverhältnismäßig und deshalb rechtswidrig." Dafür spiele es keine Rolle, dass Betroffene nicht namentlich genannt werden. Es handele sich um „eine umfangreiche Vorratsdatenübermittlung" von sensitiven Gesundheitsdaten. Geringer einschneidende Maßnahmen zum Schutz der Bewohner von Pflegeheimen seien möglich gewesen. Auch Frederick Richter von der Stiftung Datenschutz äußerte Zweifel an den Rechtsgrundlagen: „Wenn personenbezogene Daten an diverse private Einrichtungen verteilt werden, kann das unnötige Risiken für die Rechte der Betroffenen haben. Es muss geprüft werden, ob die Rechtsgrundlage eine solch großflächige Verteilung von Beschäftigtendaten an private Einrichtungen tatsächlich erlaubt." Die Kontaktnachverfolgung sei allein Sache der Gesundheitsämter (Mueller-Töwe, Eklat um Tönnies-Adressliste – Ministerium ordnete Verteilung an, www.t-online.de 29.06.2020).

### Nordrhein-Westfalen

## Alte Krankenhaus-Patientenakten frei zugänglich

Ein Video auf dem Youtube-Kanal „ItsMarvin" über offenbar unzureichend gesicherte Patientenakten in einer verlassenen Klinik in Büren hat für viel Wirbel gesorgt. Unter dem Titel „Lostplaces: Unglaublich! Dieses Krankenhaus ist zehn Jahre zu" ist seit dem 29.05.2020 zu sehen, wie der Youtuber ein Krankenhaus durch eine unverschlossene Gebäudetür betritt und sein Begleiter dort frei in Patientenakten und Röntgenbildern blättern kann. Die Polizei ermittelt seitdem nach eigenen Angaben mit Hochdruck, wie ein Sprecher am 03.06. mitteilte. Die Stadt nahe Paderborn zeigte sich empört. Bürens Bürgermeister Burkhard Schwuchow (CDU) kritisierte es als „in keinster Weise akzeptabel", dass schützenswerte Personendaten aus Patientenakten des ehemaligen St. Nikolaus-Hospitals nicht vor einem unbefugten Zugriff gesichert gewesen seien. Dass dort „sensible Akten weder sachgerecht noch datenschutzkonform aufbewahrt wurden, war der Stadt Büren nicht bekannt".

Auf der Homepage der Stadt heißt es weiter, die Klinik sei in kirchlicher, danach ab 2005 bis zur insolvenzbedingten Schließung 2010 in privater Trägerschaft der Marseille Kliniken AG (MK) gewesen. Die Verantwortung liege bei der Eigentümerin der geschlossenen Klinik, so der Bürgermeister: „Die beiden Räume, in denen die Patientenakten aufbewahrt sind, wurden am Samstag auf Initiative der Stadt und im Beisein der Polizei so verschlossen, dass niemand an die Akten gelangen kann, ohne einen erheblichen Aufwand zu betreiben." Das habe man gemacht, um die vertraulichen Patientendaten so schnell wie möglich vor „fremden Händen zu schützen", alles weitere sei nun Sache des Eigentümers. Eigentümer ist die Grundstücksgesellschaft Nikolaus Büren, die ihrerseits wieder der Marseille-Kliniken AG gehört.

Der Anwalt des Krankenhausbetreibers teilte aber mit, verantwortlich sei der Insolvenzverwalter. Nach der Insolvenz der Tochter der MK-Kliniken habe der beauftragte Bielefelder Insolvenzverwalter Norbert Westhoff die Aufgabe erhalten, in der Klinik Inventar auszubauen und zu verkaufen. „Auch die Krankenakten gehören zum Inventar der insolventen Betreibergesellschaft. Für deren ordnungsgemäße Entsorgung und Lagerung ist der Insolvenzverwalter verantwortlich". Dieser sei aufgefordert worden, dafür nun auch Sorge zu tragen.

Die Polizei hat gemäß eigenen Angaben in dem Fall eine Strafanzeige wegen des Verdachts auf Hausfriedensbruch erhalten. Es werde aber auch geprüft, ob weitere strafrechtlich relevante Sachverhalte vorliegen könnten. Details nannte der Sprecher nicht – auch nicht, gegen wen sich die Ermittlungen richteten. Der 29-jährige Youtuber, der das Video gefilmt und publiziert hat, arbeitet hauptberuflich in der Werbebranche. Sein Kanal hat 465.000 Abonnenten. Er erklärte, mit seinem Video die Stadt nicht an den Pranger stellen zu wollen, doch glaube er nicht, dass diese nicht von dem frei zugänglichen Gebäude gewusst hat: „Mir haben Leute geschrieben, dass sie sich an die Stadt gewandt hatten. Es ist doch schade, dass die Bürger offenbar einen besseren Draht zu mir haben als zum Bürgermeister." Auch mit dem Eigentümer der verlassenen Klinik habe er Kontakt. Dieser habe ihm versichert, keine rechtlichen Maßnahmen gegen ihn ergreifen zu wollen (Ungesicherte Patientenakten in Büren: Polizei ermittelt, www.sueddeutsche.de 03.06.2020; Hunderte Patientenakten, frei zugänglich, SZ 04.06.2020, 8).

### Sachsen

## Verfassungsschutzchef wegen Weigerung des Datenlöschens versetzt

Nachdem sich der Chef des sächsischen Landesamtes für Verfassungsschutz (LfV) Gordian Meyer-Plath geweigert hatte, Daten zu AfD-Rechtsaußen-Abgeordneten zu löschen, wurde er vom Innenminister des Freistaats Roland Wöller (CDU) ins Wissenschaftsministerium versetzt. Acht Jahre lang war Meyer-Plath Chef des sächsischen Verfassungsschutzes. Linken war der konservative Geisteswissenschaftler und „Alte Herr" einer Burschenschaft stets suspekt, immer wieder warfen sie ihm vor, zu wenig gegen Rechtsextremismus zu unternehmen. Nun verlor er seinen Job, offenbar wegen genau dem Gegenteil, nämlich weil er angeblich zu forsch gegen mögliche Rechtsextremisten in den Reihen der AfD vorging. An die Spitze des Verfassungsschutzes in Sachsen rückt mit Dirk-Martin Christian nun ausgerechnet jener Jurist aus dem Innenministerium, der Meyer-Plath als Referatsleiter im Innenministerium und damit als Aufsicht gebremst hatte. Wöller erklärte wegen der erfolgenden öffentlichen Diskussion: „Die Indiskretionen sind haltlos." Es sei Anzeige wegen Verrat von Dienstgeheimnissen erstattet worden.

Der Vorgang sorgt auch in den ande-

ren deutschen Verfassungsschutzämtern für Aufregung, wo man nicht nachvollziehen kann, warum Sachsen beim Umgang mit der AfD ausschert, zumal der dortige Landesverband maßgeblich vom sogenannten „Flügel" geprägt wird. Das Bundesamt für Verfassungsschutz (BfV) hat die völkische AfD-Strömung im Frühjahr 2020 als „erwiesen extremistisch" eingestuft. In einem vertraulichen BfV-Gutachten wurden mehrere AfD-Politiker aus Sachsen als „Flügel"-Anhänger benannt, darunter Landes- und Fraktionschef Jörg Urban und der Bundestagsabgeordnete Jörg Maier.

Das Innenministerium in Dresden befand jedoch, dass das LfV Daten zu insgesamt acht AfD-Abgeordneten löschen muss, darunter die zu Bundesparteichef Tino Chrupalla; Mandatsträger seien besonders geschützt. Behördenchef Meyer-Plath weigerte sich, weil dadurch der Freistaat „in einem der dynamischsten Felder des modernen Rechtsextremismus" seine „Arbeit einstellen" würde, wie er in einem Schreiben warnte.

Im Innenausschuss des Landtags rechtfertigte Sachsens Innenminister Wöller am 02.07.2020 das Vorgehen seines Hauses. Teilnehmer der Sitzung berichten, der Minister habe seinen Geheimdienst dort „in den Senkel gestellt". Das Amt habe rechtswidrig Daten über AfD-Abgeordnete gesammelt. Gegenüber der Aufsicht im Innenministerium habe sich der Dienst beratungsresistent gezeigt und die Speicherung nur unzureichend begründet. Dies habe zu der Weisung geführt, die Datensammlung zu löschen. Der neue Geheimdienstchef Christian erklärte: „Man kann nicht die Verfassung schützen und selbst Verfassungsbruch begehen". Hintergrund ist das Ramelow-Urteil des Bundesverfassungsgerichts von 2013. Der Linken-Politiker stand jahrelang auf der Beobachtungsliste des Verfassungsschutzes (DANA 1/2014, 45 f.). Christian meinte, Abgeordnete müssten ihre Aufgabe frei von staatlicher Kontrolle ausüben können. Der Demokratie sei nicht gedient, wenn Menschen auf Verdacht und ohne Rechtsgrundlage beobachtet würden.

Der Grünen-Innenpolitiker Valentin Lippman sprach von einem „ungeheuerlichen Vorgang". Der sächsische Verfassungsschutz habe sich „offenbar verselbständigt und mit verfassungsrechtlich fragwürdigen Methoden gearbeitet. Der Fall zeigt einmal mehr, dass Einiges im Landesamt für Verfassungsschutz im Argen liegt." Seine Partei regiert in Sachsen mit. Auch wenn er hier das Geschäft der AfD betreibe, so Lippmann, sei es „richtig gewesen, dass die Fachaufsicht hier eingeschritten ist". Die Linke-Innenexpertin Kerstin Köditz hatte nach der Sitzung den Eindruck, der Verfassungsschutz sei „zu dämlich" gewesen, das Speichern der Daten von AfD-Abgeordneten zu begründen. Über Innenminister Wöller meinte er: „Er ist für das Landesamt für Verfassungsschutz verantwortlich und sieht seit Jahren dabei zu, wie es beim Kampf gegen Rechts herumstümpert."

Für die AfD ist der Vorgang ein gefundenes Fressen; sie empörte sich umgehend über eine „illegale Bespitzelung". Dabei teilt keines der anderen Verfassungsschutzämter die restriktive Auffassung des Dresdner Innenministeriums. Bei der Frage, wann Daten über Abgeordnete erhoben werden dürfen, orientieren sich die Dienste bundesweit an einem einheitlichen Schema. Verfassungsschützern außerhalb Sachsens war schon länger aufgefallen, dass Meyer-Plath der Rückhalt seines Ministeriums fehlte, er wohl gern mehr gegen die neuen Formen des Rechtsextremismus unternehmen wollte, aber nicht durfte (Schmid/Winter/Wiedmann-Schmidt, Ausgebremst, www.spiegel.de, 02.07.2020; Nimz, Sächsische Prüffälle, SZ 03.07.2020, 6).

## Schleswig-Holstein

## Datenschützerin Hansen rehabilitiert und wiedergewählt

Die Leiterin des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) Marit Hansen hat in einem Verfahren beim Oberlandesgericht Schleswig (OLG) durch Urteil vom 26.06.2020 Wiedergutmachung gegen die Staatsanwaltschaft Kiel bzw. das Justizministerium Schleswig-Holstein erlangt (Az. 17 EK 2/19). Hintergrund sind fast vier Jahre dauernde, 2019 eingestellte strafrechtliche Ermittlungen wegen mutmaßlichen Betrugs bei der Abrechnung von Projektfördermitteln. Hansen warf der Staatsanwaltschaft vor, das im Oktober 2015 eingeleitete Verfahren verzögert und ihr persönlich wie der Dienststelle des ULD geschadet zu haben. Die Ermittlungen seien „von Pleiten und Pannen" geprägt gewesen. Das OLG gab ihr inhaltlich vollumfänglich Recht. Am 18.06.2020, also kurz vor der OLG-Entscheidung, wurde Hansen einstimmig vom Landtag Schleswig-Holstein für eine zweite Amtsperiode wiedergewählt. Durch ein Konkurrentenverfahren wurde zunächst ihre Ernennung durch den Ministerpräsidenten mit einer einstweiligen Anordnung des Verwaltungsgerichts Schleswig (VG) verhindert.

### Ex-Mitarbeiter provoziert Ermittlungsverfahren

Schon der Umstand, dass aufgrund einer dünnen einseitigen Verdächtigung eines ehemaligen ULD-Mitarbeiters vom Amtsgericht auf Antrag der Staatsanwaltschaft ein Durchsuchungsbeschluss in der unabhängigen Datenschutzbehörde initiiert worden war, ist wohl einzigartig in der Geschichte des Datenschutzes in Deutschland. Bei der Durchführung der Durchsuchung waren Datenbestände mitgenommen worden, deren Beschlagnahme von dem Gerichtsbeschluss nicht gedeckt gewesen war. Der zuständige Staatsanwalt habe, so Hansens Vorwurf, zwei Zeugen ohne Aussagegenehmigung vernommen. Eine wichtige entlastende Information wurde mehr als 11 Monate nicht zu den Akten genommen. Die Ermittler hatten sich durch die Anzeige des gekündigten ULD-Mitarbeiters auf eine falsche Spur bringen lassen, so Hansen: „Der Anfangsverdacht beruhte auf gravierenden Fehlinformationen."

Die Vorwürfe Hansens werden durch die Überprüfung der ULD-Abrechnungspraxis durch das Bundesforschungsministerium (BMBF) gestützt sowie durch eine Entscheidung des Amtsgerichts Kiel, das der ULD-Chefin vom Grunde her einen Entschädigungsanspruch zubilligte. Das OLG rehabilitierte nun die Datenschutzbeauftragte.

### Hansen fordert Aufklärung und Entschuldigung

Die 50-jährige Diplom-Informatikerin Hansen sah sich durch die 44 Monate

langen Ermittlungen, über die in den Medien berichtet worden war, in ihrem Ruf beschädigt und die Arbeit des ULD beeinträchtigt. Mit ihrer Klage, die sich formal gegen das zuständige Justizministerium des Landes richtete, wurde ihr vom OLG bestätigt, dass die Dauer des Verfahrens unangemessen war und dies der Staatsanwaltschaft auch bewusst war: „Eine Strafverfolgungsbehörde in einem Rechtsstaat darf Ermittlungen nicht verschleppen". Sie ist auch darüber verärgert, dass die Staatsanwaltschaft in der Begründung der Verfahrenseinstellung die Möglichkeit einer geringen Schuld offengelassen hat: „Alle Abrechnungen waren sauber, und das ist auch belegt."

Ende Oktober 2015 hatte der Ex-Mitarbeiter des ULD Strafanzeige gegen die Datenschutzbeauftragte erstattet und ihr sowie einem weiteren ULD-Mitarbeiter vorgeworfen, bei der Abrechnung von öffentlich geförderten Forschungsprojekten betrogen zu haben. Arbeitszeiten und Auslagen seien als projektbezogen angegeben und abgerechnet worden, obwohl sie es nicht gewesen seien. Hansen habe Mitarbeitende aufgefordert, Zeiten und Auslagen falsch zu erfassen. Mit diesen unzutreffenden Aufwänden hätten dann Hansen und ihrer Mitarbeiter zu Unrecht Fördergelder für das ULD erschlichen. Die Staatsanwaltschaft nahm einen Anfangsverdacht an und erwirkte den richterlichen Beschluss, der es Ermittlern des Landeskriminalamtes und der Staatsanwaltschaft ermöglichte, im ULD eine Razzia durchzuführen und Akten und Datenträger zu beschlagnahmen. Danach wurde das Verfahren nicht weiterbetrieben. Die ULD-Chefin legte viermal erfolglos hiergegen Beschwerde ein. Dreimal wechselte im Laufe der zuständige Staatsanwalt. Hansen, die auch beruflich darunter gelitten hatte, erklärt: „Die lange Zeit war sehr frustrierend für mich und meine Familie."

**Die OLG-Entscheidung**

Das OLG bestätigte, dass das Ermittlungsverfahren gegen Hansen und ihren Mitarbeiter mit seiner Dauer wie seiner inhaltlichen Ausgestaltung unangemessen war. Damit war deren Anspruch auf eine effektive und der Unschuldsvermutung gerecht werdende Verfahrensgestaltung verletzt worden. Es habe keine zielgerichtete Verfahrensplanung gegeben, obwohl das Verfahren wegen der frühzeitig erfolgten Durchsuchung hätte beschleunigt durchgeführt werden müssen. Ihre Forderung nach einer finanziellen Kompensation wies das OLG mit dem Argument zurück, Hansen habe sich im Vor- und Nachgang schon angemessen medial darstellen können. Dem ULD-Mitarbeiter wurde ein Schadenersatzanspruch von 1.800 € zugesprochen.

**Staatsanwaltschaft und Politik**

Die Angelegenheit hat eine hohe politische Brisanz: Das ULD ist unabhängige Datenschutzaufsichtsbehörde für die Staatsanwaltschaft und die Ministerien. Die Staatsanwaltschaft ist nicht nur in diesem Fall ins Gerede gekommen, weil sie sich immer wieder dem Verdacht aussetzt, politisch zu agieren und sich gar politisch instrumentalisieren zu lassen. Der Grünen-Innenpolitiker Burkhard Peters erinnerte: „Ich denke da zum Beispiel an die Ermittlungen gegen die ehemalige Bildungsministerin Wara Wende oder an die frühere Kieler Oberbürgermeisterin Susanne Gaschke, die sofort mit einem Strafverfahren überzogen wurden. Die Ermittlungen gingen mit großem Getöse los. Am Ende blieb davon nicht viel übrig." Wende und Gaschke gehören der SPD an. SPD-Fraktionschef Ralf Stegner erinnert an Durchsuchungsaktionen im Regierungsviertel „mit großem Blendwerk", die ohne Ergebnis endeten, aber den Ruf der zu Unrecht Beschuldigten ruiniert hätten. Aktuell steht die von Brigitte Heß geleitete Staatsanwaltschaft in Kiel wieder im Fokus eines politischen Konfliktes, bei dem es um Konflikte in der Polizei des Landes geht und die jüngst dem bisherigen Innenminister Hans-Joachim Grote das Ministeramt kosteten und der Polizeibeauftragten Samiah El Samadoni eine Dienstaufsichtsbeschwerde und einen Strafantrag gegen Unbekannt einbrachte, weil Inhalte aus einem Vieraugengespräch mit ihr bei einem Polizeigewerkschafter gelandet waren. Polizeibeamte hatten sich zuvor wegen Mobbings an El Samadoni gewandt; Grote hatte es sich zur Aufgabe gemacht, die Landespolizei zu reformieren. Das ULD ist nun aufgefordert, die Umstände des Grote-Rücktritts datenschutzrechtlich zu durchleuchten. Dabei geht es u.a. um die Weitergabe sog. Bestra-Berichte und um eine mögliche Verletzung des Briefgeheimnisses.

Zu den Vorwürfen einer politisierenden Strafverfolgung wollte sich die Staatsanwaltschaft selbst nicht äußern: Sie nehme nicht an politischen Diskussionen teil. Die Landesvorsitzende des Richterverbands Christine Schmehl nannte dagegen die Vorhaltungen einen „Schlag ins Gesicht" für viele Mitarbeiter in der Strafverfolgung und „Wasser auf den Mühlen von Verschwörungstheoretikern".

Erst zum Ende des inzwischen eingestellten Strafverfahrens hatte die Staatsanwaltschaft auf Nachfrage dem angeblich geschädigten Bundesforschungsministerium die Ermittlungsakten zur Verfügung gestellt. Dort gab man eine vertiefte Prüfung der Fördermittelverwendung in Auftrag. Ein dreiköpfiges Prüfteam aus Berlin war im Oktober 2019 mehrere Tage vor Ort und durchleuchtete die Abrechnungen zahlreicher Projekte. Ergebnis: keinerlei Fehler, schon gar nicht irgendein Betrug. Hansen zeigte sich frustriert darüber, dass dieser Sachverstand nicht frühzeitig genutzt wurde: „Dann hätten sich die Vorwürfe schnell aufklären lassen." Es könnten Fehler gemacht werden: „Aber dann muss man auch dazu stehen und sich möglicherweise entschuldigen." Dafür sieht man bei der Staatsanwaltschaft keine Veranlassung. Das Verfahren, so Oberstaatsanwalt Henning Hadeler, sei „stets angemessen gefördert" worden. Die Dauer begründet er mit dem „besonderen Umfang" durch die notwendige Vernehmung zahlreicher Zeugen und Sachverständiger, zeitintensiver Auswertetätigkeit bei der Polizei sowie der Schwierigkeit der Rechtslage.

**Hansen gewählt und nicht ernannt**

Nachdem sich die OLG-Entscheidung inhaltlich schon anlässlich der mündlichen Verhandlung abgezeichnet hatte, war Hansen auf Vorschlag der FDP-Fraktion am 18.06.2020 einstimmig von Landtag Schleswig-Holstein wiedergewählt worden, ohne dass Ministerpräsident Daniel Günter (CDU) sie im Anschluss ernennen konnte. Ihre erste Amtszeit endete nach den Berechnungen der Landtagsverwaltung Mitte Juli 2020. Das

Gesetz sieht vor, dass sie ein halbes Jahr nachdienen darf, so dass eine Ernennung bis Mitte Januar für eine ununterbrochene Tätigkeit möglich ist.

Grund für die ‚Verzögerung ist eine einstweilige Anordnung, die einer der zwei weiteren Bewerbenden beim VG Schleswig beantragt hatte. Bei dem Antragsteller handelt es sich um den ehemaligen ULD-Mitarbeiter, der das 44-monatige Strafverfahren gegen Hansen initiiert hatte. FDP-Fraktionschef Christopher Vogt kommentierte die gerichtliche Intervention: „Wir sehen der Konkurrentenklage gelassen entgegen." Er habe den Eindruck, dass der Kläger „nicht in der Liga von Frau Hansen spielt". Der FDP-Jurist Jan Marcus Rossa meinte, dass es sich bei der Position der Landes-Datenschutzbeauftragten nicht um ein öffentliches Amt im Sinne des Grundgesetzes handele, sondern um ein Wahlamt: „Wahlämter haben eigene Regeln." Garantiert werden müsse ein transparentes Verfahren. Eine Fraktion schlägt den Bewerber vor, das Parlament wählt ihn, die Regierung spricht die Ernennung aus. Die Landesregierung müsse sich innerhalb der Frist äußern. Derweil zeigte sich Hansen mit ihrer Wahl zufrieden: „Das Gericht hat nicht die Wahl gestoppt. Die Wahl war so eindeutig, dass es klar ist, was das Parlament möchte" (Marit Hansen gewählt, aber noch nicht ernannt, Kieler Nachrichten – KN – 19.06.2020, 11; Metschies, Oberste Datenschützerin verklagt das Land, KN 23.05.2020,12; Holbach, Die Staatsanwaltschaft und die Politik, KN 16.05.2020, 14; Pressemitteilung OLG Schleswig Nr. 6/2020 v. 26.06.2020).

### Thüringen

## Hasse spricht von Bußgeldern gegen Lehrer wegen unerlaubtem Softwareeinsatz

Der Thüringer Datenschutzbeauftragte Lutz Hasse hat wegen möglichen Verstößen von Lehrkräften gegen den Datenschutz beim Digitalunterricht während der Corona-Krise von Bußgeldern von bis zu 1.000 Euro gesprochen und sich dadurch viel öffentliche Kritik eingehandelt. Hasse erklärte, ihn hätten „Hinweise erreicht" zur Verwendung von nicht zugelassener Software oder Kommunikationsplattformen. Es geht um die Frage, welche Software, Cloudspeicher und Plattformen Lehrkräfte nutzen dürfen. Hasse nannte als Negativbeispiel Whatsapp und wollte „aus wettbewerblichen Gründen" keine weiteren Namen nennen. Gemeint sind wohl Videodienste wie Zoom oder Microsoft Teams oder private Gmail-Konten, über die Schüler und Lehrer kommunizieren.

In Thüringen gibt es eine Schulplattform, über die zum Beispiel Hausaufgaben hochgeladen werden können. Zudem verfügen Lehrer über spezielle E-Mail-Postfächer. Wenn ein Lehrer darüber hinaus andere digitale Werkzeuge verwenden will, muss er eigentlich bei der Schulleitung eine Genehmigung einholen. Die wiederum muss beim zuständigen Ministerium anfragen. Und in jedem Fall muss der Datenschutzbeauftragte die Sicherheit dieser Werkzeuge prüfen. Lutz Hasse: „Während des digitalen Unterrichts haben uns diesbezüglich mehr als 30 Anfragen von Lehrern und Schulen erreicht." Auch in Zeiten wie diesen, so Hasse, sei man eben an geltendes Recht gebunden.

Trotzdem müsse jetzt kein Lehrer befürchten, dass ihn einfach so ein Bußgeldbescheid erreicht. Zunächst müsse geprüft werden, ob der Fehler beim einzelnen Lehrer oder bei der Schulleitung liege. Und dann würde er zunächst das Gespräch suchen, um den Sachverhalt aufzuklären: „Aber ich kann als Datenschutzbeauftragter eben auch nicht beide Augen zudrücken."

Bildungsminister Helmut Holter (LINKE) bezeichnet das Vorgehen Hasses als beunruhigend und nicht akzeptabel. Eine Verunsicherung von Lehrern sei der schlechteste Weg zu guter Bildung und zu gutem Datenschutz. Datenschutzbedenken sollten gemeinsam geklärt werden. Von einem Schlag ins Gesicht engagierter Lehrerinnen und Lehrer sprach die Gewerkschaft Erziehung und Wissenschaft Thüringen (GEW). Die GEW-Landesvorsitzende, Kathrin Vitzthum, forderte vom Datenschutzbeauftragten, die Pädagogen zu beraten, statt Bußgelder zu prüfen. Von einem völlig falschen Signal in die Lehrerschaft sprach auch die Thüringer Landeselternvertretung. Die aktuelle Situation erfordere ein Miteinander, kein Gegeneinander, Konzepte statt Schuldzuweisungen, Unterstützung statt Verunsicherung.

Ähnlich äußerte sich der Bildungsexperte der CDU-Landtagsfraktion, Christian Tischner. Lehrern mit Bußgeldern zu drohen und sie dadurch zu verunsichern, sei definitiv der falsche Weg. Bei den flächendeckenden Schulschließungen im März habe es zunächst keine landesweite Plattform für den digitalen Unterricht gegeben. Das Engagement und die Kreativität im Nachhinein zu bestrafen, sei ganz und gar kontraproduktiv. Es war von einer „Hexenjagd auf Lehrerinnen und Lehrer" die Rede. Ähnlich die FDP-Fraktion im Landtag. Deren bildungspolitische Sprecherin, Franziska Baum, forderte vom Bildungsministerium praxistaugliche Anleitungen zum Datenschutz für den Digitalunterricht und damit Rechtssicherheit für Lehrer und Eltern. Es könne nicht sein, dass die Verantwortung an dieser Stelle bei den Lehrern hängen bleibt. Der Bildungsausschuss des Landtags befasste sich umgehend mit dem Thema. Der Bundesdatenschutzbeauftragte Ulrich Kelber hielt es für eine „Selbstverständlichkeit, dass ein Landesdatenschutzbeauftragter seinem gesetzlichen Auftrag nachkommt" und Hinweisen nachgehe. Die Aufregung, dass es bei unverhältnismäßigen Verstößen auch Bußgelder geben könnte, sei unbegründet (Kritik nach Androhung von Bußgeldern gegen Lehrer, www.mdr.de 04.06.2020; Hurtz, Bittere Lektion, SZ 06./07.06.2020, 9).

### Aufgespießt

## Datenfreiheit für Kommunarden!

Der 79jährige Ex-Kommunarde Rainer Langhans plädierte für das freizügige Teilen persönlicher Daten im Internet: „Gebt alle Daten frei." Wer ängstlich über seine Daten und sein Eigentum daran wache, sei wie jemand, der auf seinem Geld sitze: „Leider haben die Leute noch immer Angst vor der Freiheit, vor der Liebe." Das Internet biete hier eine neue Dimension: „Die höchste Form der Kommunikation ist Liebe. Der besitzbefreite große Datenverkehr miteinander ist Liebe" (SZ 15.06.2020, 8).

# Datenschutznachrichten aus dem Ausland

### Weltweit

## Oracle-Tracking-Datenbank öffentlich im Netz

Eine Tracking-Datenbank der Oracle-Tochter BlueKai mit persönlichen Informationen und Profilen auch deutscher Webnutzer stand offen im Netz. Weitgehend unbemerkt von der Öffentlichkeit verfolgt der Datenbankkonzern die Spuren von Online-Nutzern und baute so ein umfangreiches Tracking-Netzwerk auf. Die massive Datenpanne gab nun Einblicke in die entsprechenden Aktivitäten des Konzerns aus dem Silicon Valley. Die Panne hat der Sicherheitsforscher Anurag Sen entdeckt. Auf einem ungesicherten, ohne Passwort zugänglichen Server stieß der Experte auf ein Verzeichnis mit Milliarden personenbezogener Datensätze, die für jedermann offen einsehbar waren.

Sen hat Oracle über seinen brisanten Fund informiert, die klaffende Sicherheitslücke ist der Firma zufolge geschlossen. Gemäß Recherchen der Presse, die Zugang zu der Datenbank hatte, enthielt diese Namen, Anschriften, E-Mail-Adressen und andere personenbeziehbare Daten von Nutzern aus aller Welt. Darunter seien auch sensible Browsing-Verläufe gewesen, die von Shopping-Touren im Web bis zu Abbestellungen von Newsletter-Abonnements reichten.

Bennett Cyphers von der US-Bürgerrechtsorganisation Electronic Frontier Foundation (EFF) erklärte: „Man kann es kaum beschreiben, wie aufschlussreich einige dieser Daten sein können.“ Fein abgestufte Aufzeichnungen über die Surfgewohnheiten von Menschen im Web könnten Hobbys, politische Vorlieben, Einkommensklassen, den Gesundheitszustand, sexuelle Präferenzen und andere persönliche Details offenbaren. Die Aussagekraft nehme ständig zu, „da wir einen immer größeren Teil unseres Lebens online verbringen“. Die umfangreichen, als nicht-pseudonymisierte Rohdaten nach außen gedrungenen Nutzerspuren hat Oracle dem Bericht nach vor allem über seine Tochter BlueKai zusammengetragen. Das Unternehmen hatte das Start-up 2014 für gut 400 Millionen US-Dollar gekauft. Obwohl es außerhalb von Marketingkreisen kaum bekannt ist, hat es mithilfe von Cookies und anderen Tracking-Instrumenten wie Schnüffelpixeln auf Webseiten inklusive Porno-Portalen und in HTML-Mails einen großen einschlägigen Werbeverbund aufgebaut. Auf dem zugehörigen Markt für Profiling und personenbezogene Werbung gelten Google mit seinem Netzwerk DoubleClick, Facebook und Amazon als noch größere Datensammelmaschinen.

Die Zeitschrift TechCrunch sprach angesichts der schieren Größe der exponierten Datenbank von einer der bislang „größten Sicherheitslücken in diesem Jahr“. Man habe darin sogar Aufzeichnungen mit Einzelheiten über teils sehr private Online-Einkäufe gefunden, die bis August 2019 zurückreichten. In einem Datensatz werde detailliert beschrieben, wie ein namentlich identifizierter Deutscher am 19.04.2020 eine Prepaidkarte benutzt habe, um ein 10-Euro-Gebot auf einer Website für E-Sports-Wetten zu platzieren. Die Aufzeichnungen sollen auch die Adresse, Telefonnummer und E-Mail des Mannes umfasst haben. Als weiteres Beispiel nennt das Magazin Einträge einer der größten türkischen Investmentfirmen. Darüber habe sich etwa zurückverfolgen lassen, dass ein Nutzer aus Istanbul für 899 US-Dollar Möbel bei einem Online-Ausstatter erstanden habe. Interessenten unter anderem für Dashcams seien ebenfalls leicht persönlich ausfindig zu machen gewesen.

Nach kalifornischem Recht und der Datenschutz-Grundverordnung (DSGVO) ist Oracle verpflichtet gewesen, die zuständigen Aufsichtsbehörden über das Leck binnen enger Fristen zu informieren. Dem Bericht nach versäumte der Konzern dies aber bislang. Die DSGVO sieht bei Verstößen Bußgelder bis zu 20 Millionen Euro beziehungsweise vier Prozent des Jahresumsatzes eines Unternehmens vor.

Laut Branchenexperten verfolgt BlueKai rund 1,2% des gesamten Datenverkehrs im Web und arbeitet mit den Betreibern einiger der größten Homepages und Online-Dienste wie Amazon, ESPN, Forbes, Levi's, MSN.com, Rotten Tomatoes und der New York Times zusammen. Sogar in dem TechCrunch-Artikel war ein BlueKai-Tracker eingebaut, weil die Muttergesellschaft Verizon Media zu den Partnern der Firma gehört. Letztlich setzt fast jede Medienseite, die sich ganz oder teils über Werbung finanziert, auf einschlägige Verfahren zur Nutzeranalyse. Hierzulande betonten die Datenschutzaufsichtsbehörden erstmals vor zwei Jahren, dass Tracker wie Google Analytics und Cookies selbst in pseudonymisierter Form nur mit ausdrücklicher und informierter Einwilligung der Nutzer erlaubt sind. Die von Anwendersystemen abgegriffenen Daten und daraus geformten Profile würden längst nicht nur für Anzeigen verwendet, beklagte der Bundesdatenschutzbeauftragte Ulrich Kelber im Jahr 2019 (Krempl, Oracle: Datenpanne mit Milliarden Einträgen enthüllt riesiges Tracking-Netz, www.heise.de 21.06.2020, Kurzlink: https://heise.de/-4790339.

### Europa

## NGOs kritisieren Umsetzung der DSGVO

Zwei Jahre nach dem Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) zog der Dachverband der europäischen Datenschutzorganisationen European Digital Rights (EDRi) eine erste, sehr durchwachsene Bilanz. Die Umsetzung der Verordnung in vielen Mitgliedsstaaten sei völlig ungenügend und systematische Verstöße blieben vielfach ungeahndet. In Staaten wie Ungarn, der Slowakei und Rumänien würden die Datenschutzbehörden politisch instrumentalisiert, um gegen Medienberichte vorzugehen.

Am 25.05.2020 warf zudem Max Schrems (noyb) der irischen Datenschutzbehörde (DPC) vor, mit Facebook zur Umgehung der Datenschutzgesetze regelrecht zu konspirieren. Die DPC

agiere quasi als fünfte Kolonne der US-Internetkonzerne, deren Europazentralen fast alle in Irland niedergelassen sind. Max Schrems: „Seit Jahren hören wir von den nationalen Datenschutzbehörden immer dieselben schönen Worte über eine effizientere Umsetzung der DSGVO, über bessere Koordination und europäische Zusammenarbeit gegen die Umgehungspraktiken der Internetkonzerne. Passiert ist aber nichts. Irgendwann haben uns diese schönen Worte gereicht. Es ist jetzt einmal Zeit, Tacheles zu reden. Die Herrschaften sollen bitte auch einmal öffentlich sagen, ob sie die DSGVO denn überhaupt durchsetzen wollen. In Irland hat das nämlich überhaupt nicht den Anschein, vielmehr sieht das nach Sabotage aus."

Der irischen Datenschutzbehörde wird von Schrems vorgeworfen, in zehn gemeinsamen Sitzungen mit Facebook einen Plan ausgearbeitet zu haben, mit dem die in der DSGVO vorgeschriebene Zustimmung durch die Benutzer umgangen wird. Am Tag des Inkrafttretens der DSGVO in Irland war der Begriff „Zustimmung" aus den Geschäftsbedingungen des Sozialen Netzwerks verschwunden. Stattdessen beruft sich Facebook auf einen ominösen „Datennutzungsvertrag" mit den Benutzern, der Facebook Datenverarbeitungen aller Art erlaube bzw. den Konzern sogar dazu verpflichte. Die irische Datenschutzbehörde akzeptiert diese Vorgangsweise des Internetkonzerns bis heute als legitim.

noyb hat vor zwei Jahren drei Verfahren gegen Facebook, Instagram und WhatsApp – alle drei gehören zum Facebook-Konzern – gestartet. 22 Monate brauchte die Behörde allein, um die Vorwürfe gegen Facebook in erster Instanz zu prüfen. Wenn die Verfahren in diesem „Tempo" weitergehen, könne es zehn Jahre dauern, bis einer dieser Prozesse abgeschlossen wird. Zuletzt waren Dating-Apps wie Tinder wegen inflationärer Datenweitergaben ins Visier der Datenschützer geraten. Schrems: „Das ist ganz einfach juristische Rosstäuscherei. Seit dem Römischen Recht ist es verboten, einen gesetzlich geregelten Vorgang umzubenennen, um die Regelung zu umgehen. Die gesamte Vorgehensweise der Irischen Datenschutzbehörde ist einfach kafkaesk." Derselbe Punkt steht auch auf der Beschwerdeliste von EDRi ganz oben, nämlich Missbrauch der Zustimmungsregelung, indem die Benutzer zur Zustimmung für Datenweitergaben en Gros genötigt werden.

Es sei nun höchste Zeit, dass die nationalen Datenschutzbehörden diesem „Business as usual"-Treiben der Internetkonzerne durch die Umsetzung der DSGVO ein Ende setzten, fordern die Bürgerrechts- und Datenschutzorganisationen. Dazu brauche es adäquate finanzielle, technische und personelle Kapazitäten für die nationalen Datenschützer, damit diese überhaupt gegen die in jeder Beziehung überlegenen Internetkonzerne vorgehen könnten. Das sei leider in kaum einem Mitgliedsstaat der Fall. Es sei daher nun höchste Zeit, dass die Kommission gegen diese Staaten Verfahren einleite, da die Umsetzung der Verordnung dadurch hintertrieben werde.

Die jeweiligen Mitgliedsorganisationen des EDRi-Dachverbands haben Missbrauchsfälle ausführlich dokumentiert. Demgemäß ist das europäische Gesamtbild alarmierend. Zwei der von European Digital Rights dokumentierten Beispiele des Missbrauchs der DSGVO zu politischen Zwecken stammen aus jüngster Zeit. So hatte die slowakische Datenschutzbehörde das tschechische Zentrum für investigativen Journalismus mit einer Strafandrohung von zehn Millionen Euro (!) Ende 2019 dazu zwingen wollen, ein Video vom Netz zu nehmen. Das Video zeigt den mittlerweile verhafteten slowakischen Unternehmer Marian Kocner, wie er eine Überwachungskamera im Büro des ehemaligen Generalstaatsanwalts Dobroslav Trnka installiert, der in Folge ermordet wurde. Kocner sitzt wegen dieses und der Morde an den Journalisten Jan Kuciak und Martina Kusnirova in Untersuchungshaft.

In Ungarn hatte einer der Oligarchen, die Viktor Orban im Sattel halten, unter Berufung auf die Datenschutz-Grundverordnung eine einstweilige Verfügung gerichtlich durchgesetzt, die Februar-Ausgabe des US-Wirtschaftsmagazins „Forbes" beschlagnahmen zu lassen. Einer der Eigentümer des größten ungarischen Getränkekonzerns wollte partout nicht in der Liste der 50 reichsten Ungarn aufgeführt werden. In Rumänien wiederum wurde Ende 2018 versucht, einen Bericht des Anti-Korruptionsprojekts RISE über den Missbrauch von EU-Geldern in Rumänien zu verhindern. Auch diese Intervention lief über die Datenschutzbehörden, auch hier wurde versucht, die Berichterstatter durch die (theoretisch möglichen) hohen Strafen gegen Datenschutzverstöße einzuschüchtern.

Gemäß EDRi ist aus den letzten 25 Jahren keine weitere EU-Verordnung bekannt, die so breit und systematisch hintertrieben wurde, wie dies aktuell mit der DSGVO der Fall ist. In jedem anderen Fall war bei vergleichbaren Tatbeständen der Nicht-Umsetzung einer EU-Verordnung oder Richtlinie, ein Verfahren der Kommission gegen den betreffenden Staat die Folge. Mit der DSGVO wird, so der Vorwurf, regelrecht Schindluder getrieben (Moechel, Datenschutz-NGOs frontal gegen Datenschutzbehörden, 31.05.2020, https://fm4.orf.at/stories/3003167/)

**Europa**

## Kelber: EDSA soll Datenschutzverfahren zentralisieren

Der Bundesdatenschutzbeauftragte Ulrich Kelber hat sich dafür ausgesprochen, große Datenschutzverfahren auf die europäische Ebene zu ziehen und dort zu verfolgen: „Auf Dauer wäre es sinnvoll, wenn der Europäische Datenschutzausschuss wichtige, grenzüberschreitende und ressourcenfressende Fälle an eine europäische Serviceeinheit übertragen könnte, die ihm zugeordnet ist. Das würde eine deutliche Beschleunigung bringen. Hintergrund ist, dass etwa bei den irischen Datenschützern seit Mai 2018 elf Untersuchungen gegen Facebook laufen, davon aber bisher keine abgeschlossen worden ist. Der Europäische Datenschutzausschuss (EDSA) besteht aus Vertretern der nationalen Datenschutzbehörden und dem Europäischen Datenschutzbeauftragten.

Die „Serviceeinheit" sollte laut Kelber „auf keinen Fall eine Institution der EU-Kommission sein". Denn die jetzigen Datenschutzbehörden seien alle unabhängig. „Die Stelle müsste die gleiche

Unabhängigkeit haben." Um nicht in nationales Recht einzugreifen, wäre es daher sinnvoll, sie an den Europäischen Datenschutzausschuss anzugliedern. „Der Ausschuss könnte die Institution dann beauftragen, zum Beispiel mit einer 80-Prozent-Mehrheit."

Mit Blick auf die Datenschutz-Grundverordnung (DSGVO) zog Kelber eine positive Bilanz. Mit der Umstellung der Verfahren habe es natürlich „Anlaufschwierigkeiten" gegeben: „Es gab teilweise absurde Panikmache aus Sensationsgier, wegen Clickbaiting, aus Unkenntnis, aber auch durch Versuche, Geschäftsmodelle damit zu verbinden. Trotzdem haben wir die wesentlichen Ziele erreicht. Wir haben eine Harmonisierung in der EU, wir haben ein gesteigertes Bewusstsein für Datenschutz und wir haben bessere Durchsetzungsmöglichkeiten." Die deutschen Datenschutzbehörden sähen in neun Bereichen Verbesserungsbedarf an der DSGVO. „Wir sind zum Beispiel der Meinung, dass der Grundsatz ‚Privacy by design' auf die Hersteller von Produkten ausgeweitet werden sollte." Dann beginne der „Datenschutz durch Technikgestaltung" schon eine Stufe früher als heute. Zudem habe man auch Vorschläge zur Praxistauglichkeit gemacht, etwa bei den Informationspflichten (Datenschutz: Kelber will große Datenschutzverfahren auf EU-Ebene übertragen, wallstreet-online.de 24.05.2020).

**Österreich**

## Personenregister jahrelang öffentlich zugänglich

Ein Register mit persönlichen Daten von einer Million Bürgerinnen und Bürgern, also gut 11% der Gesamtbevölkerung, war auf einer österreichischen Ministeriums-Website jahrelang einsehbar. Aufgefallen war die Datenbank mit Namen, persönlichen Adressen und Geburtsdaten durch die Abwicklung von Anträgen aus dem Corona-Härtefallfonds. Laut Wirtschaftsministerium war das Register seit elf Jahren öffentlich einsehbar. In dem inzwischen aus dem Netz genommenen Register wurden laut den liberalen Neos und der Datenschutzorganisation epicenter.works, die das Leck am 08.05.2020 öffentlich machten, unter anderem Bundespräsident Alexander Van der Bellen, Ex-FPÖ-Chef Heinz-Christian Strache, rund 100 Nationalratsabgeordnete, namhafte Schauspieler und sonstige Prominente genannt. Das Wirtschaftsministerium wies darauf hin, dass die gegenwärtige Umsetzung des Ergänzungsregisters in einer Verordnung von 2009 geregelt sei. Das Register sei öffentlich zu führen. Erfasst sind darin u.a. Selbständige, die unter dem Vereins- und Firmenregister nicht aufgeführt sind. Die Regierung hatte die Datenbank 2004 öffentlich eingerichtet. Es sei ursprünglich bei der Datenschutzkommission, der späteren Datenschutzbehörde, angesiedelt gewesen und Ende 2018 dem Wirtschaftsministerium übertragen worden. Man stehe einer rechtlichen Anpassung und Verbesserung jederzeit offen gegenüber. Das System wurde vom Netz genommen.

Die Bürgerrechtler von epicenter.works sprachen von einem „Geschenk der Republik an jeden Datenhändler und Identitätsdieb". Es sei nicht ersichtlich, wieso das Register mit Stammzahlen öffentlich für jeden hürdenfrei abrufbar sein sollte: „Daher ist die Grundrechtseinschränkung ungerechtfertigt." Die Verordnung sei vermutlich verfassungswidrig, könnte aber grundsätzlich noch solange angewendet werden, bis sie der Verfassungsgerichtshof gegebenenfalls aufhebe. Die ÖVP, der Wirtschaftsministerin Margarete Schramböck angehört, verwies auf die Verantwortung der Vorgängerregierungen und sprach von „künstlicher Aufregung" (Millionen Daten einsehbar, SZ 09./10.05.2020, 8; Krempl, Sensible Daten von rund einer Millionen Bürger jahrelang offen im Netz, www.heise.de 09.05.2020, Kurzlink: https://heise.de/-4717831).

**Slowakei**

## Verfassungsgericht stoppt Corona-Handy-Überwachung

Das Verfassungsgericht Kaschau der Slowakei hat am 13.05.2020 entschieden, dass die Gesundheitsbehörden des Landes vorerst nicht mehr die Handydaten ihrer Bürger gegen deren Willen überwachen dürfen. Unter Verweis auf die Corona-Pandemie wurden die Bewegungen aller Handy-Benutzer erfasst. Die höchste juristische Instanz der Slowakei gab damit einer Beschwerde der oppositionellen Sozialdemokraten gegen eine Ende März 2020 beschlossene Novelle des Telekommunikationsgesetzes teilweise Recht. Die von der konservativ-populistischen Parlamentsmehrheit beschlossene Gesetzesnovelle hatte der obersten staatlichen Gesundheitsbehörde den Zugriff auf die Handy-Standortdaten der Mobilfunkbetreiber erlaubt, um damit zu verfolgen, wo sich mit dem neuartigen Coronavirus Infizierte bewegen und mit wem sie sich treffen.

Oppositionspolitiker begrüßten die Entscheidung der höchsten Richter. Der sozialdemokratische Vizeparteichef und ehemalige Gesundheitsminister Richard Rasi erklärte, die Gesetzesnovelle sei mit dem Ausmaß ihres Eingriffs in Datenschutz und Bürgerrechte „beispiellos in Europa" gewesen. Allerdings ist die Gesetzesnovelle nicht aufgehoben, sondern nur vorläufig außer Kraft gesetzt worden. Grund für diese Entscheidung war keine grundsätzliche Verfassungswidrigkeit von Handyüberwachung, sondern dass Zweck, Dauer und Kontrolle der außerordentlichen Maßnahme nicht ausreichend definiert worden sind. Von der Entscheidung nicht betroffen ist eine von der Regierung zusätzlich geplante App, mit der die Einhaltung verpflichtender Quarantäne bei Corona-Verdacht überwacht werden soll. Die slowakischen Sozialdemokraten setzen sich auch gegen diese Form der Überwachung zur Wehr (Verfassungsgericht der Slowakei stoppt Mobilfunk-Überwachung, www.heise.de 14.05.2020, Kurzlink: https://heise.de/-4720905).

**Slowakei**

## App-Kontrolle ersetzt Quarantäne-Lager

Wer aus dem Ausland in die Slowakei einreist, muss nicht mehr zwingend in eines der umstrittenen staatlichen Quarantäne-Zentren. Das Parlament in Bratislava stimmte am 15.05.2020 der von der Regierung am Vortag beschlos-

senen Einführung einer Handy-App zur freiwilligen Überwachung zu: Wenn sich Rückkehrer aus dem Ausland die App auf ihr Smartphone installieren lassen, dürfen sie die vorgeschriebene 14-tägige Quarantäne auch zuhause verbringen. Sobald sie aber ihre Wohnung verlassen, wird ein Alarmsignal an die Behörden gesendet. Gemäß dem konservativen Gesundheitsminister Marek Krajci geht die unter dem Namen „intelligente Quarantäne" eingeführte Alternative umgehend in den Wirkbetrieb, um die überfüllten Quarantäne-Zentren zu entlasten.

Die Slowakei weist eine der niedrigsten Infektionsraten mit dem Coronavirus in Europa auf. Bis Mitte Mai 2020 verzeichnete das 5,4 Millionen Einwohner zählende Land nur 1480 bestätigte Infektionsfälle und lediglich 27 Corona-Tote. Während die Regierung diese im Vergleich zu allen Nachbarländern außerordentlich günstigen Zahlen als Erfolg ihrer radikalen Schutzmaßnahmen rühmte, machte sich in Teilen der Bevölkerung Unmut breit. Ombudsfrau Maria Patakyova und verschiedene Bürgerinitiativen kritisierten vor allem die staatlichen Quarantäne-Zentren, in die Heimkehrer nach dem Grenzübertritt gebracht wurden. Die an Gefangenenlager erinnernde Unterbringung widerspreche der in der Verfassung und in internationalen Konventionen garantierten Menschenwürde, klagten sie (Covid-19: Slowakei ersetzt Staatsquarantäne durch Handy-App, www.heise.de 16.05.2020, Kurzlink: https://heise.de/-4722661).

### Israel

## Geheimdienst sucht wieder Corona-Kontaktpersonen

In der Nacht zum 21.07.2020 verabschiedete das israelische Parlament ein Gesetz, das den Inlandsgeheimdienst Schin Bet bis ins Jahr 2021 hinein ermächtigt, Handydaten und andere sensible Informationen zu nutzen, um Menschen ausfindig zu machen, die mit Corona-Infizierten in engerem Kontakt waren. Wer auf diese Weise aufgespürt wird, muss umgehend für zwei Wochen in Quarantäne. In der Praxis wurden diese Überwachungsmethoden, die zuvor nur zum Aufspüren und Verhindern möglicher Terrorakte eingesetzt wurden, mit einer kurzen Unterbrechung bereits seit Ausbruch der Pandemie im März genutzt. Datenschützer und Bürgerrechtler sind von Beginn an dagegen Sturm gelaufen. Sie fürchten bei dieser Massenüberwachung nicht nur das Erstellen kompletter Bewegungsprofile, sondern auch den direkten Zugriff auf Inhalte in sozialen Netzwerken und E-Mails. Sogar der Schin-Bet-Chef Nadav Argaman zeigte sich höchst unzufrieden damit, von der Regierung für solch eine „zivile Angelegenheit" eingespannt zu werden. Es gibt offenkundig erhebliche Probleme mit der Treffgenauigkeit der Überwachung, wie das Gesundheitsministerium einräumte. Demnach sind allein in der ersten Juli-Hälfte mehr als 150.000 Israelis in Isolation geschickt worden wegen eines vermeintlichen Kontakts mit einem Corona-Infizierten. Rund 30.000 erhoben Einspruch dagegen; 58% von ihnen wurden daraufhin aus der Quarantäne entlassen.

Der Regierung von Premierminister Benjamin Netanjahu, die sich wegen ihrer sprunghaften Anti-Corona-Politik unter Druck befindet, setzt dennoch mit aller Macht auf den Geheimdienst. Im März 2020 war dessen Überwachungsauftrag per Notverordnung und mit dem Plazet des Generalstaatsanwalts eingeführt worden. Im April hatte jedoch das Oberste Gericht bestimmt, dass ein solch fundamentaler Eingriff in die Privatsphäre der Bürger einer entsprechenden Gesetzgebung bedarf (DANA 2/2020, 82).

Dies schien dann zwischenzeitlich wegen der gesunkenen Infektionszahlen nicht mehr nötig zu sein. Doch mit dem Ausbruch der zweiten Welle wurde zuerst die Schin-Bet-Überwachung reaktiviert und dann das geforderte Gesetz verabschiedet. Vorgesehen sind in diesem auch ein paar Einschränkungen. So ist der Einsatz des Geheimdienstes nur erlaubt, solange es pro Tag mehr als 200 neue Infizierte gibt. Ende Juli 2020 waren bis zu knapp 2.000 neue Fälle verzeichnet worden. Zudem wurde das Gesundheitsministerium aufgefordert, eine verbesserte Version der Open-Source-Kontaktapp namens Magen 2 – auf Deutsch: Schutzschild 2 – schnellstens auf den Markt zu bringen.

Sie soll die Privatsphäre besser schützen, ihr Einsatz ist freiwillig. Geheimdienstminister Eli Cohen merkte an, dass diese App den Schin-Bet-Einsatz frühestens dann ersetzen könnte, wenn sie von einem Drittel aller israelischen Smartphone-Besitzer genutzt wird. Die Bürger des Landes verlieren immer mehr den Überblick, was im Kampf gegen Corona noch erlaubt und was bereits verboten ist. Der zuständige Parlamentsausschuss revidierte mehrere von der Regierung erlassene Maßnahmen: Strände und Schwimmbäder sollen entgegen zunächst ausgesprochenen offiziellen Verboten an Wochenenden geöffnet bleiben. Restaurants, deren Schließung angeordnet worden war, bekamen schon wenige Stunden später die Erlaubnis, weiterhin Gäste bewirten zu dürfen (Münch, Agenten im Einsatz gegen Corona, SZ 22.07.2020, 7).

### USA

## GEDmatch-Gendatenbank kompromittiert

Bei der Genealogie-Datenbank GEDmatch konnten Ermittler auf Profile zugreifen, die für sie tabu sein sollten. Mit der Genealogie-Datenbank GEDmatch laden Fans der Ahnenforschung DNA-Informationen hoch, um so Verwandte ausfindig zu machen. Am 19.07.2020 waren wichtige Voreinstellungen für die sensiblen Gendaten von über einer Million Profile so verändert worden, dass sie plötzlich von Strafverfolgern für Abgleiche mit Kriminalitätsdatenbanken verwendet werden konnten.

Der Vorfall ist ein Rückschlag für die Bemühungen des GEDmatch-Mutterunternehmens Verogen, Anwender von der Strategie zu überzeugen, dass der Datenbankanbieter ihre Privatsphäre schützt und zugleich der Polizei einen partiellen kommerziellen Zugang zu Profilen auf freiwilliger Basis gewährt. Das Unternehmen für forensische Genetik will auf Basis dieses Ansatzes Geld verdienen und zugleich helfen, Gewaltverbrechen mithilfe von Genealogie aufzuklären.

Wenn Nutzer dies zulassen und ihr Profil entsprechend markieren, können Ermittler über den Dienst Personen fin-

den, die genug DNS mit einem Verdächtigen teilen, deren Genspuren Fahnder in Verbindung mit einem Verbrechen bereits sichergestellt haben. Strafverfolger hatten mithilfe von GEDmatch 2018 Joseph James DeAngelo festgenommen (DANA 2/2018, 116 f.). Sie gingen davon aus, dass es sich bei dem Ex-Cop um den „Golden State Killer" handelte. Der Verhaftete bekannte sich vorigen Monat zu 13 Morden und Dutzenden anderer Verbrechen schuldig, die größtenteils schon Jahrzehnte zurücklagen. Die Ermittler kamen DeAngelo auf die Spur, indem sie DNA des Mörders auf die Genealogie-Datenbank hochluden und ein gefälschtes Profil für ihn anlegten. Für eine Stammbaumanalyse reichen dort auch Daten weiter entfernter Verwandter und Vorahnen, sodass darüber bereits große Teile der US-Bevölkerung identifiziert werden können.

Eigentlich haben bei GEDmatch nur rund 280.000 von 1,45 Millionen Nutzern per ausdrücklichem Opt-in zugestimmt, dass ihre Profile von Fahndern in Suchaktionen nach Kriminellen einbezogen werden dürfen. Verogen erklärte die unerwünschte Offenlegung der Daten auch der anderen Mitglieder für diesen Zweck mit einer „ausgefeilten Attacke auf einen unserer Server über ein bestehendes Nutzerkonto". Der Angreifer habe in Folge sämtliche Benutzerrechte zurückgesetzt, wodurch alle Profile für alle Mitglieder sichtbar geworden seien. Nach etwa drei Stunden sei der Fehler behoben worden.

Nach dem Hack nahm der Dienst zunächst wieder seine Arbeit auf. Einen Tag später kam es laut der Genealogin CeCe Moore von der Firma Parabon NanoLabs, die eng mit der Polizei bei der Verbrechensaufklärung zusammenarbeitet, aber zu einem zweiten Vorfall: Diesmal waren demnach alle Suchmöglichkeiten für Ermittler gesperrt und Forschungsprofile sichtbar, die eigentlich gar nicht in Datenabgleiche einbezogen werden sollen.

Verogen nahm das Portal daraufhin vom Netz mit dem Hinweis auf Wartungsarbeiten. Man habe Anzeige erstattet, arbeite mit einer Cybersicherheitsfirma zusammen und führe eine umfangreiche forensische Untersuchung durch, um die Schutzmaßnahmen zu verbessern. Nutzerdaten seien nicht heruntergeladen oder kompromittiert worden. An dieser Behauptung kamen aber Zweifel auf, so warnte die israelische Genealogieseite MyHeritage ihre Kunden vor einem gezielten Phishing-Angriff auf Nutzer, die auch ein Konto bei GEDmatch haben. Wer auf einschlägige Links in Mails klicke, werde zur URL myheritaqe.com umgeleitet, bei der das „g" durch ein „q" ersetzt wurde. So versuchten die Hacker, an Nutzernamen und Passwörter zu kommen, hieß es bei der Konkurrenz. Der Verdacht liege nahe, dass die Angreifer die E-Mail-Adressen und Namen für das Missbrauchsvorhaben über den GEDmatch-Hack erhalten hätten. MyHeritage erlaubt es der Polizei nicht, die eigene Gendatenbank zu nutzen (Krempl, Gendatenbank: Über eine Millionen DNA-Profile von GEDmatch enthüllt, www.heise.de 23.07.2020, Kurzlink: https://heise.de/-4851323).

### Indien

## Zwangs-App mit Hindernissen

Die Kontaktverfolgungs-Corona-App „Aarogya Setu" (Hindi: „eine Brücke zur Gesundheit") verbreitete sich in Indien zunächst schnell: Für 50 Millionen Downloads brauchte die nach Behördenangaben gerade mal 13 Tage. Premierminister Narendra Modi rief die 1,3 Milliarden Bürger seines Landes auf, sie zu installieren. Je mehr Leute mitmachten, desto besser funktioniere die App. Ähnlich wie andere Corona-Warn-Apps soll die Anwendung aus Indien dabei helfen, die Ausbreitung des Coronavirus einzudämmen. Bald nach dem Start machte die Regierung die zuerst freiwillig zu installierende Corona-App nach und nach für mehr und mehr Menschen verpflichtend. Dazu gehören Bürger, die ihr Haus verlassen, um zu arbeiten, und solche, die in vom Virus besonders betroffenen Gebieten leben, ebenso Rückkehrer aus dem Ausland sowie Zugfahrgäste. Erwischen Polizisten diese Menschen ohne App auf dem Handy, drohen Bußgelder oder Gefängnisstrafen.

Die App ist seit Anfang April 2020 auf dem Markt. Nach 6 Wochen war sie auf den Smartphones von mehr als 100 Millionen Menschen installiert, also von weniger als zehn Prozent der indischen Bevölkerung. Nach Modellen von Forschern der Universität Oxford sollten jedoch 60% einer Bevölkerung eine Kontaktverfolgungs-App nutzen, damit neue Infektionsketten wirksam erkannt und schnell unterbrochen werden können.

Wissenschaftler des Massachusetts Institute of Technology (MIT), das Corona-Tracker rund um die Welt verglichen hat, stellten fest, dass Indien die einzige Demokratie der Welt ist, die Bürger zum Herunterladen einer Corona-Kontaktverfolgungs-App verpflichtet. Diese geht zudem weiter als die Corona-Apps vieler anderer Länder, indem sie nicht nur via Bluetooth die räumliche Nähe zu anderen Smartphones feststellt, sondern via GPS auch den Ort der Begegnung auswertet. Weiterhin hat die App noch eine Einstufung in die Risikokategorien Grün, Orange und Rot, basierend auf Selbstangaben zum Gesundheitszustand und der Reisegeschichte.

In einer Kernfunktion ähneln sich die Konzepte aus Indien und Deutschland: Kommt der Nutzer in die Nähe eines anderen App-Besitzers, tauschen sie automatisch Daten aus. Wird jemand positiv auf das Virus getestet, werden die Kontakte nachträglich informiert. Laut Angaben des indischen Gesundheitsministeriums waren bisher Mitte Mai rund 140.000 Nutzende nach Kontakten mit Corona-Infizierten wegen einer möglichen Infektion gewarnt worden. Die Behörden hätten dank der Daten außerdem rund 700 Corona-Hotspots finden und darauf reagieren können. In Indien galt seit Ende März eine strikte Ausgangssperre, die nur langsam gelockert wurde. In dieser Zeit hatte sich die Corona-Kurve jedoch nicht abgeflacht.

Schon kurz nach dem Start der App fanden Hacker Sicherheitsprobleme. Der französische Sicherheitsexperte Robert Baptiste etwa wies darauf hin, dass die persönlichen Daten der Nutzer in Gefahr seien. Damit löste er größere Diskussionen auf Twitter aus. Die indische Regierung konterte, dass es kein solches Risiko gebe. Datenschützer gehen von noch mehr Schwachstellen aus, die aber unbemerkt bleiben, weil die Regierung den Quellcode der App unter Verschluss hält. Es ist gemäß Apar Gupta, dem Chef der indischen Internet Freedom Foundation, zudem unklar,

wer genau Zugriff auf die Daten hat. Er fürchtet, dass die App die Pandemie überdauern wird. Indien hat bisher weder ein nationales Datenschutzgesetz noch gibt es Regelungen, die die Regierung zwingen würden, nach der Coronakrise auf die App zu verzichten: „In außergewöhnlichen Zeiten geben Menschen viel leichter ihre Privatsphäre auf, auch für Technologien, von denen noch nicht ganz klar ist, wie viel sie tatsächlich helfen werden. Damit geben wir der Regierung immer mehr Macht, uns zu überwachen."

Einige Inder wehren sich gegen das App-Tracking. Ein Programmierer aus Bengaluru teilte mit, er habe den Code der App so verändert, dass sie weder persönliche Informationen verlange, noch seine Bewegung aufzeichne. Andere Leute hätten bei App-Kontrollen Screenshots der Apps gezeigt, bei denen die sichere Risikokategorie Grün angezeigt wird. Wieder andere Inder können die App gar nicht herunterladen; Schätzungen zufolge haben weniger als die Hälfte der 1,3 Milliarden Menschen im Land ein Smartphone (Galli, Darum hat es Indiens Anti-Corona-App trotz Nutzungspflicht schwer, www.spiegel.de 15.05.2020).

#### Hongkong

## Social-Media-Unternehmen reagieren auf Sicherheitsgesetz

Der zum Facebook-Konzern gehörende Messengerdienst Whatsapp kündigte in Reaktion auf das umstrittene neue Sicherheitsgesetz in Hongkong an, bis auf weiteres an die Hongkonger Justizbehörden keine Nutzerdaten mehr auszuhändigen. Zunächst sollen die Auswirkungen des Anfang Juli 2020 in Kraft gesetzten Sicherheitsgesetzes geprüft werden. Dazu werde es Beratungen mit Menschenrechtsexperten geben. Ähnlich äußerten sich Facebook, Google und Twitter. Auch Dienste wie Telegram, Zoom und Linkedin teilten mit, Anfragen Honkonger Behörden nach Daten vorerst nicht zu beantworten.

Das Gesetz ist der radikalste Einschnitt in die Autonomie Hongkongs, die der früheren britischen Kronkolonie bei der Übergabe an China 1997 für mindestens 50 Jahre zugesagt wurde. Es sieht lebenslange Haft als Höchststrafe für zahlreiche Vergehen vor, die Chinas Behörden als Subversion, Abspaltung und Terrorismus werten.

Derweil kündigte ein Sprecher der Video-App TikTok des chinesischen Konzerns Bytedance an, sein Angebot „angesichts der jüngsten Ereignisse" in Hongkong vom Markt zu nehmen. Das Netzwerk hatte in der Vergangenheit erklärt, man werde Zensurgesuche oder Bitten um Nutzer-Daten der chinesischen Regierung nicht Folge leisten. Die zensierte und in der Volksrepublik verfügbare chinesische Plattform-Version „Douyin" werde in der ehemals britischen Kronkolonie aber weiter betrieben. TikTok zählt zu den weltweit beliebtesten sozialen Netzwerken, steht aber wegen seines chinesischen Eigentümers Bytedance und wegen Datenschutzbedenken in der Kritik (DANA 1/2020, 57 f.). US-Außenminister Mike Pompeo hatte kurz zuvor angekündigt. ein Verbot des Dienstes zu prüfen. Nach Daten von Sensor Tower verzeichnete TikTok im September 2019 rund 1,8 Millionen Downloads in Hongkong – bei 7,4 Millionen Einwohnern. Mit dem Rückzug aus Hongkong dürfte TikTok die vorgegebene Distanz zur Volksrepublik unter Beweis stellen wollen (TikTok kündigt Rückzug aus Hongkong an – WhatsApp liefert keine Daten mehr, www.handelsblatt.com 07.07.202; WhatsApp liefert keine Daten mehr, www.sueddeutsche.de 06.07.2020 = Keine Daten für Hongkong, SZ 07.07.2020, 6; Brühl/Giesen, In der digitalen Klemme, SZ 08.07.2020, 7).

# Rechtsprechung

#### EuGH

## „Aus" für Privacy Shield und US-Datenübermittlungserlaubnis

Der Europäische Gerichtshof (EuGH) hat mit Urteil vom 16.07.2020 auch die Nachfolgeversion von Safe-Harbor, den transatlantischen Datenschutzschild (Privacy Shield) gekippt (C-311/18). Hintergrund dieses Urteils ist wieder die Klage des österreichischen Juristen und Datenschutzaktivisten Max Schrems gegen die irische Datenschutzbehörde (DPC) wegen der transatlantischen Datenübermittlungen bei der Benutzung der Social-Media-Plattform Facebook. Mit dem Privacy Shield erklärte der EuGH eine der wichtigen Rechtsgrundlagen für den Transfer personenbezogener Daten europäischer Bürger in die USA für nichtig. Grund dafür sind in den Vereinigten Staaten bestehende Gesetze, die Sicherheitsbehörden weitreichende Befugnisse zur Überwachung „ausländischer Kommunikation" in die Hand geben.

Europäische Tochtergesellschaften von US-Konzernen wie Facebook dürfen gemäß dem EuGH Datenübermittlungen grundsätzlich auf Basis des Beschlusses der EU-Kommission über Standardvertragsklauseln (SVK) persönliche Informationen an Auftragsverarbeiter in Drittländern übertragen. Ob dies tatsächlich erlaubt sei, müssen die zuständigen Datenschutzbehörden aber jeweils ausloten. Auch die SVK haben so im USA-Fall nur noch pro forma Bestand.

Der EuGH begründet seine Entscheidung damit, dass mit der Datenschutz-Grundverordnung (DSGVO) personenbezogene Daten grundsätzlich nur dann in ein Drittland übermittelt werden dürfen, wenn dieses dafür ein „angemessenes Schutzniveau" gewährleistet. Die Kommission sei befugt, einen solchen Level mit einem Beschluss festzustellen. Liege keine solche Angemessenheitsentscheidung vor, müsse der in der EU ansässige Datenexporteur selbst „geeignete Garantien" vorsehen. Diese könnten sich etwa aus den von der Kommission erarbeiteten Standard-Datenschutzklauseln ergeben. Hierfür

müssten die betroffenen Personen „über durchsetzbare Rechte und wirksame Rechtsbehelfe verfügen".

Max Schrems hatte gegenüber der irischen Datenschutzbehörde den Transfer seiner personenbezogenen Informationen durch die nationale Facebook-Tochter an den Mutterkonzern in den USA moniert und beantragt, alle Datenübermittlungen zwischen den beiden Unternehmen auszusetzen. Das Stammunternehmen sei nämlich verpflichtet, die erhaltenen Informationen etwa auf Basis von Paragraf 702 des Foreign Intelligence Surveillance Act (FISA) US-Behörden wie der NSA und dem FBI zugänglich zu machen, ohne dass die Betroffenen dagegen gerichtlich vorgehen könnten. Das Gericht nahm ausdrücklich Bezug auf NSA-Überwachungsprogramme wie Prism oder Upstream, die durch Edward Snowdens Enthüllungen 2013 bekannt geworden waren. Damit zapfen die US-Behörden Datenkabel an und greifen auf Metadaten wie auch auf Inhalte zu, ohne dass den Bürgern ein angemessener Rechtsschutz gewährt wird.

Facebook hatte dagegen geltend gemacht, dass das EU-Recht generell nicht für die Verarbeitung personenbezogener Daten für Zwecke der nationalen Sicherheit gelte. Die irische Kontrollbehörde wandte sich daraufhin an den irischen High Court, um die Rechtmäßigkeit der Transfers zu klären, die per Standardvertragsklauseln erfolgte. Die angerufenen Richter wollten daraufhin vom EuGH etwa wissen, ob die entsprechende Übermittlung die EU-Grundrechtecharta und die darin verbürgten Ansprüche auf Schutz der Privatsphäre und einen wirksamen Rechtsbehelf verletzt.

Der EuGH stellte den Beschluss der EU-Kommission über die SVK nicht völlig in Frage. Bei einer Prüfung ergebe sich nichts, was seine Gültigkeit berühren könnte. Europäisches Recht und insbesondere die DSGVO seien generell auf einen zu gewerblichen Zwecken erfolgenden Transfer persönlicher Daten anzuwenden. Dies gelte auch, wenn die Daten direkt oder im Anschluss von Behörden des betreffenden Drittlands verarbeitet werden könnten.

Personen, deren Informationen weitergesendet werden, müssen ein Schutzniveau in Anspruch nehmen können, das dem der DSGVO entspricht. Es sei Pflicht der europäischen Datenschutzbehörden wie etwa der irischen Aufsichtsstelle zu prüfen, ob diese Anforderungen erfüllt sind. Insbesondere, wenn es keinen Angemessenheitsbeschluss der Kommission gebe, seien sie dabei auch angehalten, einen Transfer „auszusetzen oder zu verbieten". Voraussetzung dafür sei ihre Auffassung, dass die Standardklauseln in dem entsprechenden Land nicht eingehalten werden und der nötige Schutz nicht anders gewährleistet werden kann. Parallel müssen auch der Datenexporteur und der Empfänger der Informationen laut dem Richterspruch vorab prüfen, ob das erforderliche Schutzniveau im betreffenden Drittland eingehalten wird. Konkret habe die Facebook-Mutter also die europäische Tochter gegebenenfalls selbst darüber zu informieren, dass die SVK mit all ihren Konsequenzen nicht eingehalten werden könnten.

EuGH-Generalanwalt Henrik Saugmandsgaard Øe hatte schon im Dezember 2018 argumentiert, die SVK seien tragfähig. Das Gericht sei auch nicht unbedingt verpflichtet, über die Gültigkeit des Privacy Shield zu entscheiden. Dessen Rechtmäßigkeit zweifelte er aber angesichts der in der EU verbrieften Grundrechte an. Der EuGH stellte insofern fest, dass dieser „den Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses und der Einhaltung des amerikanischen Rechts Vorrang" einräume. Dies erlaube Eingriffe in die Grundrechte der Personen, deren Daten in die USA übermittelt werden. Die Anforderungen an eine derartige Übereinkunft sehen die Richter nicht erfüllt, da die auf die US-Rechtsvorschriften gestützten Überwachungsprogramme „nicht auf das zwingend erforderliche Maß beschränkt sind". Den Betroffenen habe der US-Gesetzgeber auch keine Rechte verliehen, die sie gegenüber den amerikanischen Behörden gerichtlich durchsetzen könnten. Der vorgesehene Ombudsmechanismus reiche nicht aus.

Die EU-Kommission war davon ausgegangen, dass es keinen Konflikt mit den US-Gesetzen gebe. Wenn Unternehmen Daten auf Basis des Privacy Shield versenden wollten, müssten sie garantieren, die Mindeststandards des europäischen Datenschutzes einzuhalten. Schrems warf der EU-Kommission vor, dass sie die US-Überwachungsauflagen völlig falsch einschätze. Schrems hatte vor dem EuGH mit dessen Urteil vom 06.10.2015 bereits das Vorgängerabkommen „Safe Harbor" zu Fall gebracht (C-362/14). Mit dem Außerkraftsetzen des Privacy Shield wird wohl auch ein dritter Anlauf ohne grundsätzliche Reformen nicht ausreichend sein, um einen angemessenen Datenschutz für EU-Bürger zu gewährleisten.

Der eco-Verband der Internetwirtschaft hatte sich vorab besorgt gezeigt. Der Datenschutzschild zwischen der EU und den USA oder die SVK bildeten „eine unerlässliche Rechtsgrundlage für die internationale Übermittlung personenbezogener Daten". Ohne sie gebe es für diesen Zweck nur wenig Alternativen, sodass viele Unternehmen im Regen stünden. Die Folgen wären fatal: Zahlreiche transatlantische Transfers persönlicher Informationen würden über Nacht unzulässig. Die Digitalwirtschaft sei auf verlässliche und tragfähige Regeln und damit einhergehende Rechtssicherheit unbedingt angewiesen.

Schrems hoffte dagegen schon im Vorfeld auf einen Rückschlag für die auch vom Silicon Valley vorangetriebene „Überwachungskultur" und eine umfassende Novelle der ihr zugrundeliegenden Gesetzesklauseln. Um Daten ausländischer Nutzer zu erhalten, müsse es im Sinne die US-Industrie sein, grundlegende Schutzbestimmungen einzuführen. In den Vereinigten Staaten gebe es ja auch Bedenken, dass Informationen über US-Bürger nach China gingen, wenn diese Dienste von Huawei oder TikTok verwendeten.

**• Reaktionen**

Die öffentlich geäußerten Lesarten des Grundsatzurteils sind trotz seiner Eindeutigkeit unterschiedlich. Für Schrems, der den Stein mit einer Beschwerde über die Praktiken Facebooks bei der irischen Datenschutzbehörde DPC ins Rollen gebracht hat, steht fest: Standardvertragsklauseln „können auch nicht mehr von Facebook und US-Unternehmen genutzt werden, die unter US-Überwachung stehen". Nur wenn es kein kollidierendes Recht gebe, seien SVK noch einsetzbar. In Fällen wie bei

Facebook hätte die DPC den Betreiber des sozialen Netzwerks laut dem Juristen „schon vor Jahren anweisen können, die Datentransfers zu stoppen". Stattdessen habe sich die Behörde an den EuGH gewandt, um die – nun im Prinzip für gültig befundenen – SVK aufheben zu lassen. Sie habe die Feuerwehr gerufen aus Unlust, eine Kerze auszublasen. Der seit sieben Jahren anhängige Fall habe allein die DPC fast drei Millionen Euro gekostet. Dies zeige auch grundlegende Mängel bei der Durchsetzung der DSGVO auf. Trotz des Urteils könnten absolut notwendige Datentransfers gemäß Art. 49 DSGVO weiterhin stattfinden, heißt es bei noyb. Übermittlungen ließen sich auch auf eine informierte Einwilligung des Nutzers stützen, die aber jederzeit widerrufbar sei. Die USA würden einfach in den Status eines Landes ohne besonderen Zugang zu EU-Daten zurückversetzt.

Die in Luxemburg im Kern gescheiterte DPC begrüßte die Entscheidung ebenfalls nachdrücklich. Ihr seien Datentransfers in die USA schon nach dem Aus für das Vorgängerabkommen Safe Harbor 2015 überaus problematisch erschienen, unabhängig von der genutzten Rechtsgrundlage. Durch das Urteil sehe man die eigenen Bedenken nun voll bestätigt. Dass der EuGH das SVK-Instrument trotzdem nicht direkt verworfen habe, erfordere angesichts der Komplexität der Materie noch eine gründliche Analyse. Der SVK-Mechanismus erscheine in Bezug auf die USA nach wie vor „fraglich". Man wolle nun gemeinsam mit den „europäischen Kollegen" eine gemeinsame Position erarbeiten.

Der Bundesdatenschutzbeauftragte Ulrich Kelber verwies auf eine nun bestehende große Herausforderung. Unternehmen, die öffentliche Verwaltung und die in ihrer Rolle gestärkten Aufsichtsbehörden „haben jetzt die komplexe Aufgabe, das Urteil praktisch anzuwenden". Die Kontrollinstanzen müssten „bei jeder einzelnen Datenverarbeitung" prüfen, „ob die hohen Anforderungen des EuGH erfüllt werden". Internationaler Datenverkehr bleibe zwar generell weiter möglich. Dabei seien aber die Grundrechte der EU-Bürger zu beachten. Für den Austausch mit den USA müssten nun „besondere Schutzmaßnahmen ergriffen werden".

Der Hamburgische Datenschutzbeauftragte Johannes Caspar zog ein skeptischeres Fazit: „Für den internationalen Datenverkehr ziehen schwere Zeiten auf. Die Umetikettierung des im Jahr 2015 für ungültig erklärten Vorgängerinstruments Safe Harbor mit nur marginalen Verbesserungen hat zu keinem Umdenken in der Regierung der USA geführt". Weder hätte der dortige Gesetzgeber bei der Praxis der anlasslosen Massenüberwachung etwas geändert, noch seien Betroffenenrechte substanziell gestärkt worden. Die Entscheidung, die Standardvertragsklauseln prinzipiell beizubehalten, sei nicht konsequent. Wenn primär mit den ausufernden Geheimdienstaktivitäten in den USA argumentiert werde, müsse dies für das alternative Instrument genauso gelten. Der EuGH habe den Ball den europäischen Aufsichtsbehörden zugespielt, sagte Caspar. Die Datenschutzbeauftragten in Deutschland und Europa müssten sich schnell verständigen, „wie mit Unternehmen umgegangen wird, die nun unzulässigerweise weiter auf das Privacy Shield setzen". Dasselbe gelte für Firmen, die SVK für Transfers in die USA und in andere Drittstaaten nutzten. Dabei werde sich etwa auch bei China oder Großbritannien mit Blick auf den Brexit „die Frage der zulässigen Datenübermittlung stellen". Auch der Thüringer Datenschutzbeauftragte Lutz Hasse meinte, er wisse nicht, wie im Fall von Transfers in die USA noch „ein EU-datenschutzkonformes Prüfergebnis zustande kommen soll".

Der IT-Verband Bitkom monierte, dass zum zweiten Mal eine der Rechtsgrundlagen für transatlantische Datentransfers weggefallen sei. Auch die Praxis der Standardvertragsklauseln gerate ins Wanken, es entstünde massive Rechtsunsicherheit. Wer bislang allein auf das Privacy Shield gebaut habe, müsse auf andere Verfahren umstellen, sonst „droht ein Datenchaos". Ähnlich besorgt zeigte sich der eco-Verband der Internetwirtschaft. Der Bundesverband IT-Mittelstand vermag der Entscheidung auch etwas Gutes abzugewinnen: Sie könne „den Weg dahin ebnen, dass Datensicherheit als Wettbewerbsvorteil für Europa erkannt wird". Betroffen sieht Philippe Heinzke, Rechtsanwalt bei der Wirtschaftskanzlei CMS, vor allem kleine und mittlere Unternehmen, die bislang vielfach keine Standardverträge abgeschlossen hätten. Microsoft meinte, gewerbliche Kunden dürften die Dienste des Unternehmens im Einklang mit dem europäischen Recht weiterhin nutzen: „Das Urteil des Gerichtshofs ändert nichts daran, dass Sie heute Daten zwischen der EU und den USA über die Microsoft-Cloud übertragen können." Man biete den Kunden seit Jahren einen überlappenden Schutz im Rahmen der SVK und des Privacy Shield.

Die EU-Kommission setzt nun offenbar vor allem auf eine Modernisierung der SVK. EU-Kommissions-Vizepräsidentin Vera Jourová signalisierte, dass sie sich in den USA deutlich strengere Datenschutzvorschriften zumindest für EU-Bürger wünschen würde – aber die EU könnten US-Gesetze nicht ändern: „Wir werden auf Grundlage des heutigen Urteils eng mit unseren amerikanischen Kollegen zusammenarbeiten." Justizkommissar Didier Reynders unterstrich, SVK seien bereits das gebräuchlichste Mittel für internationale Datentransfers. Man arbeite hieran bereits seit einiger Zeit. Er nannte aber keine Details. Man werde alles tun, um das Urteil vollständig umzusetzen.

Das Urteil „ist ein Sieg für die Privatsphäre gegen die Massenüberwachung", freute sich Diego Naranjo von der Initative European Digital Rights (EDRi). Die USA müssten die Arbeit ihrer Geheimdienste nun dringend reformieren. Moritz Körner, innenpolitischer Sprecher der FDP im EU-Parlament sprach von einem „Erdbeben für den internationalen Datenaustausch". Dank des Richterspruchs dürfe die Datenschnüffelei der USA nicht länger ignoriert oder hingenommen werden. Es sei traurig, „dass dies nur durch die Klage der Privatperson Schrems erreicht werden konnte" (Krempl, EuGH kippt EU-US-Datenschutzvereinbarung „Privacy Shield", www.heise.de 16.07.2020, Kurzlink: https://heise.de/-4845204; Krempl, Aus fürs Privacy Shield: Der internationale Datenverkehr kommt ins Trudeln, www.heise.de 16.07.2020, Kurzlink: https://heise.de/-4846000; Janisch, Gericht verbietet Datentransfer in die USA, SZ 17.07.2020, 1).

### Conseil d´Etat/Frankreich

## CNIL-Google-Bußgeld in Höhe von 50 Mio. € bestätigt

Das oberste französische Verwaltungsgericht, der dortige Conseil d´Etat (Staatsrat), hat am 19.06.2020 die Beschwerde von Google gegen das Bußgeldverfahren der nationalen Datenschutzbehörde, der Commission Nationale de l'Informatique et des Libertés (CNIL) zurückgewiesen. Google muss in Frankreich gemäß der CNIL-Entscheidung vom Januar 2019 wegen undurchsichtiger Privatsphäre-Einstellungen und der fehlenden rechtlichen Grundlage für personalisierte Werbung mit 50 Millionen Euro die bislang höchste Strafe zahlen, die europäische Aufsichtsbehörden auf Basis der Datenschutz-Grundverordnung (DSGVO) verhängten (DANA 1/2019, 45).

Das oberste französische Verwaltungsgericht akzeptierte die Einwände von Google gegen die Sanktion in seinem Beschluss nicht. Der US-Internetkonzern hatte unter anderem darauf abgestellt, die CNIL sei gar nicht zuständig, da sich der eigene europäische Hauptsitz in Irland befinde. Laut dem in der DSGVO verankerten „One-Stop-Shop-Prinzip" müsse der Fall an die irische Datenschutzbehörde gehen, die als konzernfreundlich und ressourcenschwach gilt und binnen anderthalb Jahren zunächst nur einen vagen Bericht zu laufenden Beschwerden gegen Facebook, Instagram und WhatsApp verfasst hat.

Der Staatsrat bestätigte, dass die CNIL zum maßgeblichen Zeitpunkt befugt war, das Bußgeld gegen Google zu verhängen. Die fraglichen Entscheidungen gingen nämlich nicht auf das Konto der irischen Niederlassung, sondern auf das der Stammfirma „Google LLC", die in den USA ansässig ist. Daraus folge, dass das in der DSGVO vorgesehene System der einheitlichen Anlaufstelle nicht anwendbar und die CNIL so zum Handeln berechtigt gewesen sei. Die Behörde habe dabei den neuen europäischen Rechtsrahmen so angewendet, wie dies vom Europäischen Datenschutzausschuss vorgegeben wurde.

Der Suchmaschinenbetreiber hatte in seiner Berufung zudem argumentiert, sein Zustimmungsverfahren für personalisierte Werbung sorgfältig erarbeitet, möglichst transparent gestaltet und dabei die Empfehlungen der Regulierer beachtet zu haben. Die CNIL hatte dagegen beanstandet, dass die von Google eingeholte Einwilligung zur Anzeige personalisierter Werbung nicht gültig sei, da die Nutzer nicht ausreichend über das Verfahren aufgeklärt würden.

So sei die Vielfalt der beteiligten Google-Dienste wie YouTube, Google Maps oder Internet-Suche nicht ersichtlich. Es werde nicht hinreichend deutlich, wie der Konzern erhobene Daten verarbeite und für wie lange er sie speichere. Die Informationen dazu seien über mehrere Dokumente verteilt, Nutzer müssten sich über diverse Links und Buttons durch das Material klicken. Der Conseil d'Etat konstatierte dazu, dass die CNIL auch die Schlüsselprinzipien der DSGVO rund um die Bereiche Transparenz, Information der User und die Notwendigkeit einer gültigen Zustimmung für personalisierte Werbung korrekt angewendet hat. Die höchsten Verwaltungsrichter erachteten die von der Kontrollinstanz festgestellten Unzulänglichkeiten zugleich als wesentlich für das Geschäftsgebaren Googles. An der Entscheidung gebe es so insgesamt nichts auszusetzen.

Den Fall ins Rollen gebracht hatten die Bürgerrechtsorganisationen noyb aus Österreich und La Quadrature du Net aus Frankreich mit weitgehenden Beschwerden auch gegen andere Online-Giganten. noyb-Mitgründer Max Schrems verwies als Reaktion auf die Ansage des Staatsrats darauf, dass der Geldbetrag für Google „zwar winzig" sei und die potenzielle Höchststrafe bei 3,7 Milliarden Euro gelegen hätte. Dennoch werde damit deutlich, dass DSGVO-Sanktionen „beträchtliche Summen erreichen können". Wichtig sei die Klarstellung, dass sich große US-Tech-Konzerne „nicht einfach als ‚irisch' deklarieren können", um einer angemessenen Datenschutzkontrolle zu entgehen. Google müsse die eigenen Bestimmungen für die Privatsphäre der Nutzer nun endlich überarbeiten und glasklar darlegen, was mit den gesammelten Informationen geschehe. Das bisherige übergreifende breite Opt-in-Verfahren über alle Dienste hinweg könne der Konzern nicht länger beibehalten.

Nicht ganz durchsetzen konnte sich die CNIL vor dem Conseil d'Etat mit ihren vergleichsweise strengen Richtlinien zum Einsatz von Cookies und anderen Tracking-Instrumenten. Im Kern erachtete das Gericht zwar auch diese Vorgaben als akzeptabel. Die CNIL-Vorgabe, mit der die umstrittene Praxis der „Cookie Walls" und der damit verknüpften Pauschaleinwilligung vollständig untersagt worden war, wurde vom Gericht nicht gehalten: Ein solches Verbot benötigte eine ordentliche Rechtsgrundlage und könne nicht über eine einfache Richtlinie vorgeschrieben werden. Die CNIL sicherte zu, ihre künftigen Empfehlungen entsprechend anzupassen (Krempl, DSGVO-Verstöße: Conseil d'Etat bestätigt 50-Millionen-Strafe gegen Google, www.heise.de 20.06.2020, Kurzlink: https://heise.de/-4790235).

### BVerfG

## Strategische BND-Telekommunikationsüberwachung ist verfassungswidrig

Das Bundesverfassungsgericht (BVerfG) hat in einem 141 Seiten langen Urteil vom 18.05.2020 festgestellt, dass die anlasslose Massenüberwachung des Bundesnachrichtendienstes (BND) von Ausländern im Ausland in ihrer bisherigen Form formell und inhaltlich gegen Grundrechte verstößt und dass das dafür grundlegende BND-Gesetz verfassungswidrig ist (Az. 1 BvR 2835/17). Erstmals wird vom BVerfG klargestellt, dass der deutsche Staat das Fernmeldegeheimnis und die Pressefreiheit auch im Ausland wahren muss und an das Grundgesetz gebunden ist.

**• Das Urteil**

Der Senatsvorsitzende Stephan Harbarth, der im Herbst 2016 als CDU-Bundestagsabgeordneter noch für die einschlägige Gesetzesnovelle gestimmt hatte, wies in seiner mündlichen Urteilsbegründung darauf hin, dass der BND die Telekommunikation an der Schnittstelle von Internationalisierung,

wachsender sicherheitsbezogener Herausforderungen und Digitalisierung, die auch eine zunehmende „Verwundbarkeit von Rechtsgütern" mit sich bringt, überwacht. Eine anlasslose strategische Aufklärung des Geheimdienstes unter Verzicht von Eingriffsschwellen dürfe es in diesem sensiblen Umfeld nicht geben. Nötig sei ein Verbot pauschaler globaler Überwachung. Der Gesetzgeber müsse Zwecke der Spionage klar festlegen und etwa spezifische Anforderungen an die „Bevorratung" von Daten und den Schutz von Vertraulichkeitsbeziehungen aufstellen. Nötig seien „Löschungspflichten". Beim Transfer von Informationen an ausländische Stellen bedürfe es klarer Vorgaben. Der individuelle Rechtsschutz der Betroffenen müsse durch eine ausgebaute, objektiv-rechtliche Kontrolle gewährleistet bleiben, die gerichtlich und administrativ sicherzustellen sei. Aus Grundrechtssicht besonders schwerwiegend sei die außerordentliche Streubreite der strategischen Telekommunikationsüberwachung.

Die Maßnahme sei „anlasslos gegenüber jedermann einsetzbar" und erlaube „gezielt personenbezogene Überwachungen"; objektive Eingriffsschwellen gebe es nicht: „Das Instrument erlaubt heute, tief in den Alltag hineinreichende, auch höchst private und spontane Kommunikationsvorgänge zu analysieren und zu erfassen sowie bei der Internetnutzung zum Ausdruck kommende Interessen, Wünsche und Vorlieben aufzuspüren." Andererseits versorge sie die „Bundesregierung mit Informationen für ihre außen- und sicherheitspolitischen Entscheidungen", um „sich im machtpolitischen Kräftefeld der internationalen Beziehungen zu behaupten" und „folgenreiche Fehlentscheidungen" zu vermeiden. Insoweit gehe es mittelbar zugleich darum, die demokratische Selbstbestimmung und den Schutz der verfassungsrechtlichen Ordnung zu wahren. Ein weiterer Gesichtspunkt für die „Rechtfertigungsfähigkeit" der strategischen Überwachung liege darin, dass sie durch eine Behörde vorgenommen werde, „die selbst grundsätzlich keine operativen Befugnisse hat".

Das BVerfG beschrieb in Auflagen, wie das Werkzeug grundrechtskonform ausgestaltet werden kann. Zunächst müsse der Gesetzgeber „einschränkende Maßgaben zum Volumen der für die jeweiligen Übertragungswege auszuleitenden Daten" auf- und sicherstellen, „dass das von der Überwachung abgedeckte geographische Gebiet begrenzt bleibt". Die Inlandskommunikation sowie erforderlichenfalls ein Austausch, an dem auf mindestens einer Seite Deutsche oder Inländer beteiligt sind, müsse der BND „vor einer manuellen Auswertung nach dem Stand von Wissenschaft und Technik bestmöglich" ausfiltern. Die Befugnis, Verbindungs- und Standortdaten im Rahmen der Auslandsüberwachung gesamthaft zu speichern und zu bevorraten, muss dem BVerfG zufolge „hinsichtlich der davon erfassten Datenströme begrenzt bleiben". Eine Speicherdauer von sechs Monaten dürfe nicht überschritten werden.

Die Richter fordern „besondere Anforderungen für den Schutz von Berufs- und Personengruppen, deren Kommunikation eine gesteigerte Vertraulichkeit verlangt". Ein gezieltes Eindringen in solche schutzwürdigen Vertraulichkeitsbeziehungen etwa von Rechtsanwälten oder Journalisten könne nicht schon allein damit gerechtfertigt werden, dass die angestrebten Informationen nachrichtendienstlich nützlich sind. Einen großen Wehrmutstropfen enthält das Urteil in Randnummer 198: Sofern Überwachungsmaßnahmen „ausschließlich dazu bestimmt und darauf ausgerichtet sind, der politischen Information der Bundesregierung zu dienen und eine Übermittlung der Erkenntnisse an andere Stellen prinzipiell ausgeschlossen ist, kann auf den Schutz von Vertraulichkeitsbeziehungen verzichtet werden, soweit dies erforderlich ist".

Dem Kernbereich privater Lebensgestaltung ist stärker Rechnung zu tragen. „Nicht hinreichend begrenzt ausgestaltet sind auch die angegriffenen Regelungen zur Übermittlung von Erkenntnissen der Auslandsüberwachung an andere Stellen". Soweit Daten an ausländische Dienste wie die NSA übermittelt würden, müsse der Gesetzgeber zusätzlich „eine Vergewisserung über den rechtsstaatlichen Umgang mit den Daten auf Empfängerseite vorschreiben". Der bisher einfach mitgeschickte „Disclaimer" genügt nicht. Die gesetzlichen Regeln müssen ferner „insbesondere einen Austausch von Erkenntnissen aus auf Deutschland bezogenen Überwachungsmaßnahmen ausländischer Dienste unterbinden". Ein solcher „Ringtausch" sei verfassungsrechtlich verboten. Mit „Ringtausch" wird bezeichnet, dass andere Dienste das tun, was man selbst nicht darf, z.B. die Überwachung im Inland, und man hinterher die Informationen tauscht.

Nach der BND-NSA-Selektorenaffäre verlangt der 1. Senat, dass die Suchbegriffe von den Partnerdiensten „plausibilisiert werden", um das „Ausspähen unter Freunden" oder Industriespionage zu verhindern. Der BND dürfe zudem von ihm erhobene Verbindungs- und Standortdaten nicht „unselektiert" ohne jede Kontrollmöglichkeit aus der Hand geben. Das Urteil fordert eine Kontrolle in institutioneller Eigenständigkeit. Hierzu gehörten ein eigenes Budget, eine eigene Personalhoheit sowie Verfahrensautonomie. Die zuständigen Stellen „sind personell wie sächlich so auszustatten, dass sie ihre Aufgaben wirksam wahrnehmen können". Inhaltlich müssten sie gegenüber dem BND „alle für eine effektive Kontrolle erforderlichen Befugnisse haben".

Gegen Teile des im Jahr 2016 novellierten BND-Gesetzes, das dem Auslandsgeheimdienst eine Überwachung ganzer Internetknoten und Netze erlaubt, hatten Anfang 2018 sieben insbesondere im Ausland investigativ arbeitende Journalisten, die Bereiche wie Korruption und Wirtschaftskriminalität recherchieren, Verfassungsbeschwerde erhoben. Auch die Organisation Reporters sans Frontieres und damit die Mutter des deutschen Ablegers Reporter ohne Grenzen (ROG) als juristische Person, hatte Einspruch erhoben. Unterstützt wurde die Beschwerde von der Gesellschaft für Freiheitsrechte (GFF), der Deutschen Journalisten-Union (dju), dem Deutschen Journalisten-Verband (DJV) sowie dem Netzwerk Recherche.

**• Datensauger**

Der in Karlsruhe verhandelte Streit drehte sich neben der Frage, ob das Grundgesetz auch für eine Sicherheitsbehörde im Ausland gilt, vor allem um die „strategische Fernmeldeaufklärung" des BND mit ihrem Schwerpunkt Ausland. Der Geheimdienst darf demnach

prinzipiell mit dieser „strategischen Kontrolle“ die internationale Telekommunikation mit bis zu hunderttausenden Selektoren wie Telefonnummern, E-Mail-Adressen oder Pseudonymen von Nutzern durchforsten und die Inhalte analysieren, die in diesem Datenstaubsauger hängenbleiben. Der 1. Senat des BVerfG wollte dem BND dieses Instrument nicht ganz aus der Hand schlagen. Er befand, dass es verhältnismäßig und damit verfassungsgemäß ausgestaltet werden könne. Die beanstandeten Vorschriften gelten daher bis zum Jahresende 2021 fort, um dem Gesetzgeber eine weitere Reform unter Berücksichtigung der grundrechtlichen Anforderungen zu ermöglichen.

Die „Rohmasse“ des Datenstaubsaugers ist riesig: Allein am Frankfurter Internetknoten De-Cix kann der BND täglich rund 1,2 Billionen Verbindungen ausleiten. Davon sollen nach dem Aussortieren erster IP-Adressen mit klarem regionalen Bezug zu deutschen Nutzern rund 24 Milliarden Rohdaten übrigbleiben. Im Inland dürfen die darauf angesetzten Suchbegriffe keine Identifizierungsmerkmale enthalten, mit denen sich bestimmte Telekommunikationsanschlüsse gezielt erfassen lassen. Für das Ausland gilt dies nicht. Aber auch dort sind für den BND etwa Telefonnummern deutscher Staatsangehöriger oder einer deutschen Gesellschaft tabu, solange es sich nicht um „Beifang“ handelt.

**• Schutz im Ausland**

Ausländer im Ausland galten bislang für den BND als „vogelfrei“, monierten Kritiker in den vergangenen Jahren immer wieder. Die Frage war im bisher letzten Urteil des BVerfG zur Thematik aus dem Jahr 1999 offen geblieben. So meinte etwa der Verfassungsrechtler Eggert Schwan, verletzt sei schon der allgemeine Gleichheitssatz aus Artikel 3 Absatz 1 Grundgesetz, weil es keinen sachlich zu rechtfertigenden Grund für diese auf den Unterschied zwischen Deutschen und Nichtdeutschen abstellende Ungleichbehandlung gebe. Die Verfassungsbestimmungen schützten Jedermann, also „alle Menschen“.

Zuvor hatte die Wende um 180 Grad an diesem Punkt schon der vormalige Präsident des Bundesverfassungsgerichts Hans-Jürgen Papier vollzogen. Das CSU-Mitglied hatte nach seinem Ausscheiden aus der Richterbank mehrfach erklärt, dass auch die Kommunikation im Ausland zwischen Ausländern grundrechtsgeschützt sei. Die BND-Zugriffe auf Datenaustauschpunkte wie den De-Cix bezeichnete Papier sogar als „insgesamt rechtswidrig“. Das ganze „strategische“ Konstrukt passe nicht mehr auf die Internetkommunikation.

Ex-BND-Chefs wie Gerhard Schindler oder August Hanning hatten vor dem Urteilsspruch betont, dass Deutschland einen starken, von Dritten unabhängigen Auslandsgeheimdienst brauche. Der BND habe immer wieder entscheidende Informationen über das weltpolitische Geschehen wie zum Irak-Krieg durch das Abhören von Telefonaten und das Mitlesen von Mails erhalten. Die Väter des Grundgesetzes würden sich im Grabe umdrehen, wenn etwa die Kommunikation der Taliban von Artikel 10 Grundgesetz geschützt sein solle. Aktive und frühere Geheimdienstler sahen sogar die Sicherheit Deutschland bei einer harten Entscheidung des BVerfG bedroht. Sie schlossen nicht aus, dass hinter dem Verfahren eine gezielte geheimdienstlich gesteuerte Aktion stecken könnte, um der Bundesrepublik zu schaden.

Das Urteil ist eines in Richtung internationale Gewährleistung von Menschenrechten. Anderswo sind ähnliche Verfahren anhängig. Der Europäische Gerichtshof in Luxemburg (EuGH) entscheidet voraussichtlich noch im Sommer 2020 zu den Diensten in Großbritannien, Belgien und Frankreich. Und der Europäische Gerichtshof für Menschenrechte in Straßburg (EGMR) hat eine Klage gegen den britischen Geheimdienst wegen dessen Massenüberwachung auf dem Tisch. Die Gerichtshöfe achten darauf, was andere Kollegen entschieden haben, so dass die Entscheidung aus Karlsruhe europaweite Wirkung haben kann.

**• Reaktionen**

Die Gesellschaft für Freiheitsrechte (GFF) lobte, der Richterspruch aus Karlsruhe setze „neue Standards im internationalen Menschenrechtsschutz und für die Freiheit der Presse“. Mit der Ansage, dass deutsche Behörden auch im Ausland an die Grundrechte gebunden sind, werde auch „die Glaubwürdigkeit Deutschlands in der Welt“ gestärkt. Christian Mihr, Geschäftsführer der an der Klage beteiligten Reporter ohne Grenzen, freute sich, „dass Karlsruhe der ausufernden Überwachungspraxis des Bundesnachrichtendienstes im Ausland einen Riegel vorschiebt“. Das Urteil setze neue Standards im internationalen Menschenrechtsschutz und für die Pressefreiheit. Die Bundesregierung bekomme damit die Quittung „für ihre jahrelange Weigerung, die digitale Massenüberwachung einzuhegen“. Die Linksfraktion im Bundestag fühlt sich in ihrer Kritik an der Reform des BND-Gesetzes bestärkt. Fraktionsvize André Hahn begrüßte als Mitglied des Parlamentarischen Kontrollgremiums des Bundestags (PKGr), dass den Überwachern der Überwacher elementare Informationen über Kooperationen des BND mit anderen Auslandsgeheimdiensten nicht mehr vorenthalten werden könnten. Der BND dürfe seine grundrechtswidrige Überwachungspraxis nicht bis zu einer Novelle ungeniert fortführen. Martina Renner, frühere Obfrau der Linken im NSA-Untersuchungsausschuss, konstatierte eine „schallende Ohrfeige“ für die jahrzehntelang praktizierte „Weltraumthreorie“ wie für die im BND ebenfalls angewendete „Funktionsträgertheorie“.

FDP-Fraktionsvize Stephan Thomae sieht im Urteil die Bestätigung, „dass unsere Werte und elementaren Grundrechte nicht an der Landesgrenze enden und auch in der Kooperation mit ausländischen Diensten berücksichtigt werden müssen“. Es müsse nun gewährleistet werden, „dass der BND sein Vorgehen bei der Fernmeldeaufklärung stärker begründet“. Konstantin von Notz, Vize-Fraktionschef der Grünen und stellvertretender PKGr-Vorsitzender, bezeichnete das Urteil als „wegweisend für die Arbeit von Nachrichtendiensten in der digitalen Welt und bedeutend für die Grundrechte von Millionen Menschen weltweit“. Die Enthüllungen Snowdens und die anschließende Aufklärung des Bundestags hätten die Rolle der deutschen Sicherheitsbehörden ans Tageslicht gebracht. Die Bundesregierung müsse jetzt schnell die Konsequenzen ziehen.

Klaus Landefeld, Vizechef des eco-Verbands der Internetwirtschaft, erklärte, „im Zeitalter digitaler Kommunikation" hätten die Verfassungshüter „das Fernmeldegeheimnis entschieden gestärkt" und dessen „extraterritoriale Schutzwirkung" erläutert, wonach eine „umfassende, unabhängige Kontrolle aller Maßnahmen vorab" notwendig sei.

Enttäuscht gab sich der EU-Abgeordnete Patrick Breyer, da das Gericht „anlasslose Massenüberwachung und flächendeckende monatelange Vorratsdatenspeicherung" nicht generell untersagt habe. Das Mitglied der Piratenpartei forderte zudem: „Verpflichtende Ende-zu-Ende-Verschlüsselung und wirksame Anonymität müssen unsere Sicherheit technisch gewährleisten." Frank Rieger, Sprecher des Chaos Computer Clubs (CCC), bedauerte, das Gericht habe nicht die globale BND-Spionage generell beendet. Es versuche nur, „sie in einen konkreteren rechtlichen Rahmen zu pressen".

Norbert Röttgen (CDU), Vorsitzender des Auswärtigen Ausschusses des Bundestags, meinte, die Entscheidung sei international „schwer vermittelbar". Indem das Gericht die BND-Abhörpraxis im Ausland kippe, werfe es „erhebliche Fragen an unsere strategische Operations- und Kooperationsfähigkeit auf – und das in einer Zeit, in der Aggression von außen immer komplexer wird".

SPD-Abgeordneter Uli Grötsch, der im PKGr sitzt, sieht sich bestätigt: „Grundrechte heißen so, weil sie grundlegend für Alle gelten müssen!" Es gelte nun, schnell das BND-Gesetz anzupassen und dem Geheimdienst „klare Regeln für seine Arbeit" zu geben. Die SPD-Fraktion sieht sich auch in ihrer Position bestätigt, dass die strategische Fernmeldeaufklärung „verfassungskonform ausgestaltet werden" kann. Der US-Geheimdienstenthüller Edward Snowden nannte das Urteil über seinen deutschen Anwalt Wolfgang Kaleck einen „Schritt in die richtige Richtung: Ich hoffe, dass sich andere Staaten am heutigen Gerichtsurteil ein Beispiel nehmen und dass auch internationale Standards entwickelt werden, um den Aufbau solcher Systeme zu verbieten." Snowden habe mit seinen Enthüllungen 2013 „auch eine Beweisgrundlage für Gerichte schaffen" wollen.

Die Bundesregierung befürchtete vorab, dass der BND seine Aufgaben nicht mehr erfüllen könne, wenn das Gericht dessen Internetaufklärung zu stark in die Grenzen weise. BND-Präsident Bruno Kahl hatte in der mündlichen Verhandlung im Januar die Befürchtung geäußert, der Dienst würde in einem solchen Fall auf einem Auge blind. 20 Prozent der Meldungen, die der Dienst generiere, basierten auf der strategischen Auslandsüberwachung (Krempl, Bundesverfassungsgericht schränkt BND-Massenüberwachung deutlich ein, www.heise.de 18.05.2020, Kurzlink: https://heise.de/-4723874; Krempl, BND-Urteil: Bundesverfassungsgericht stärkt das Fernmeldegeheimnis international, www.heise.de 19.05.2020, Kurzlink: https//heise.de/-4724784; Janisch, Wie man noch spionieren darf, SZ 20./21.05.2020, 5).

**BVerfG**

## Die Grenzen des Sag- und Postbaren

Die 2. Kammer des Ersten Senats des Bundesverfassungsgerichts (BVerfG) hat mit Beschlüssen vom 19.06.2020 über vier Verfassungsbeschwerden entschieden, die sich jeweils gegen strafgerichtliche Verurteilungen wegen Beleidigung richteten (1 BvR 2459/19, 1 BvR 2397/19, 1 BvR 1094/19, 1 BvR 362/18). Zwei Verfassungsbeschwerden wurden nicht zu Entscheidung angenommen, die anderen beiden hatten Erfolg.

Die Kammer nahm die Verfahren zum Anlass, die Grenzen der Meinungsfreiheit bei ehrverletzenden Äußerungen und die Reichweite des Schutzes des Persönlichkeitsrechts klarzustellen. Danach ist bei der Beurteilung, ob eine ehrbeeinträchtigende Äußerung rechtswidrig und unter den Voraussetzungen der §§ 185, 193 StGB strafbar ist, in aller Regel von einer Abwägung der widerstreitenden grundrechtlichen Interessen abhängig, die eine Auseinandersetzung mit den konkreten Umständen einer Äußerung und ihrer Bedeutung erfordert. Das BVerfG fasst die wesentlichen Kriterien zusammen, die bei dieser Abwägung von Bedeutung sein können. Nur in besonderen Ausnahmefällen und nur unter engen Voraussetzungen ist eine Abwägung entbehrlich, nämlich in den – spezifisch definierten – Fällen einer Schmähkritik, einer Formalbeleidigung oder einer Verletzung der Menschenwürde. Die Voraussetzungen solcher Fallkonstellationen, die das Gericht benennt, müssen von den Fachgerichten klar kenntlich gemacht und in gehaltvoller Weise begründet werden. Liegt ein solcher Sonderfall nicht vor, so das BVerfG, ist das Ergebnis der Abwägung nicht präjudiziert.

In zwei Verfahren hat das BVerfG die von den Fachgerichten vorgenommene Abwägung, wonach die Beeinträchtigung des Persönlichkeitsrechts die Meinungsfreiheit überwiegt, nicht beanstandet; in den anderen beiden Verfahren meinte es dagegen, dass keine hinreichende Auseinandersetzung mit den konkreten Situationen erkennbar war, in denen die Äußerungen gefallen sind.

1. Dem Verfahren 1 BvR 2397/19, in dem die Kammer die auch für die anderen Verfahren maßgeblichen Maßstäbe übergreifend zusammenfasst, liegen Äußerungen des Beschwerdeführers in einem von ihm geführten Internetblog zugrunde. Der Beschwerdeführer hatte sich 2002 von seiner damaligen Partnerin getrennt und führte anschließend vor verschiedenen bayerischen Gerichten zahlreiche rechtliche Auseinandersetzungen um das Umgangsrecht mit der gemeinsamen Tochter, das ihm ab 2012 ganz verwehrt wurde. 2016 verfasste er anlässlich einer für ihn nachteiligen Berufungsentscheidung drei weitere Einträge, in denen er unter anderem die an der Entscheidung beteiligten Richter sowie diverse andere Personen namentlich nannte, Fotos von ihnen ins Netz stellte und sie mehrfach als „asoziale Justizverbrecher", „Provinzverbrecher" und „Kindesentfremder", die Drahtzieher einer Vertuschung von Verbrechen im Amt seien, bezeichnete. Sie hätten auf Geheiß des namentlich genannten „rechtsradikalen" Präsidenten des Oberlandesgerichts offenkundig massiv rechtsbeugend agiert. Der Beschwerdeführer wurde deshalb von den Strafgerichten wegen Beleidigung zu einer Geldstrafe verurteilt. Zwar handele es sich wegen des sachlichen Bezugs und der verständlichen schweren emotionalen Situation des Beschwerdeführers

nicht um Schmähkritik. Bei einer Abwägung der widerstreitenden grundrechtlichen Interessen überwog jedoch der Ehrschutz. Die Kammer beurteilte das als verfassungsgemäß.

2. Dem Verfahren 1 BvR 2459/19 liegen Äußerungen des Beschwerdeführers in einer verwaltungsgerichtlichen Klageschrift zugrunde. Die Stadtbibliothek hatte – nach Rücksprache mit dem dortigen Rechtsamt – bei der Bestellung eines Buchs von ihm verlangt, das Bestellformular selbst auszufüllen. Der Beschwerdeführer hatte zuvor eine Fernleihgebühr für ein Buch nicht entrichtet, weil er meinte, ein anderes Buch bestellt zu haben. Schon zuvor hatte die Leiterin des Rechtsamtes in einer anderen Angelegenheit Strafanzeige gegen den Beschwerdeführer gestellt, aufgrund derer ein Strafverfahren wegen Urkundenfälschung gegen ihn eingeleitet worden war. In diesem Verfahren hatte er die Einholung eines psychiatrischen Gutachtens über deren Geisteszustand beantragt. Noch ehe über diesen Antrag entschieden worden war, erhob der Beschwerdeführer wegen des Streits mit der Stadtbibliothek Klage vor dem Verwaltungsgericht. In der Klageschrift äußerte er, „unter Berücksichtigung, ... dass in der Sache die Leiterin des Rechtsamtes R., eine in stabiler und persönlichkeitsgebundener Bereitschaft zur Begehung von erheblichen Straftaten befindlichen Persönlichkeit, deren geistig seelische Absonderlichkeiten und ein Gutachten zu deren Geisteskrankheit Gegenstand von gerichtlichen Auseinandersetzungen sind, involviert ist“, behalte er sich vor, „ein Ordnungsgeld in angemessener Höhe zu beantragen“. Aufgrund dieser Äußerung verurteilten die Strafgerichte den Beschwerdeführer wegen Beleidigung zu einer Geldstrafe. Zwar handele es sich nicht um einen Fall der Schmähkritik, da ein Sachbezug nicht völlig fehle. Die gebotene Abwägung falle jedoch zugunsten des Persönlichkeitsrechts aus. Auch dies beurteilte die Kammer als verfassungsgemäß.

3. Dem Verfahren 1 BvR 362/18 liegen Äußerungen des Beschwerdeführers im Rahmen einer Dienstaufsichtsbeschwerde zugrunde. Der als Rechtsanwalt tätige Beschwerdeführer vertrat 2015 einen Tierschutzverein, für den er vor einem Veterinär- und Lebensmittelüberwachungsamt ein Erlaubnisverfahren führte, an dessen Ende die vom Verein beantragte Erlaubnis erteilt wurde. Anschließend erhob der Beschwerdeführer eine Dienstaufsichtsbeschwerde gegen den zuständigen Abteilungsleiter, in der er die Ansicht vertrat, das Amt habe eine unglaubliche materielle Unkenntnis, langsame Bearbeitungszeiten und eine offensichtlich vorsätzliche Hinhaltetaktik in der Sache gezeigt. Nach Schilderung von aus Sicht des Beschwerdeführers kritikwürdigen Vorfällen äußerte er, nunmehr gehe es noch um die Verfahrenskosten des Vereins. Diese habe die Behörde zwar bereits formell anerkannt, es scheine aber so, als ob der zuständige Abteilungsleiter durch immer wieder neue Vorgaben letztlich die Kosten nicht erstatten möchte. Weiter hieß es, dessen Verhalten „sehen wir mittlerweile nur noch als offenbar persönlich bösartig, hinterhältig, amtsmissbräuchlich und insgesamt asozial uns gegenüber an“. Die Strafgerichte verurteilten den Beschwerdeführer daraufhin wegen Beleidigung zu einer Geldstrafe. Durch die verwendete Formulierung „persönlich“, „hinterhältig“ und „asozial“ sei es nur noch um eine konkrete Diffamierung des von ihm namentlich ausdrücklich benannten Abteilungsleiters gegangen, ohne dass dabei noch ein konkreter Bezug zur Sache erkennbar sei. Die Kammer beurteilte dies als eine Verletzung der Meinungsfreiheit.

4. Dem Verfahren 1 BvR 1094/19 liegen Äußerungen des Beschwerdeführers in einem einkommensteuerrechtlichen Festsetzungsverfahren zugrunde, in dem insbesondere die Abzugsfähigkeit der Kosten für ein gerichtliches Vorgehen gegen den Rundfunkbeitrag strittig war. Der Beschwerdeführer erhielt dabei ein Rundschreiben des nordrhein-westfälischen Finanzministers, in dem es hieß, Steuern machten „keinen Spaß, aber Sinn. Die Leistungen des Staates, die wir alle erwarten und gern nutzen, gibt es nicht zum Nulltarif“. Daraufhin verfasste der Beschwerdeführer ein weiteres Schreiben an die Finanzbehörden, das hauptsächlich die Frage der Absetzbarkeit der Kosten des rechtlichen Vorgehens gegen den Rundfunkbeitrag zum Gegenstand hatte. Am Ende erklärte er, weitere Dienstaufsichtsbeschwerden jetzt zu erheben, dürfte sinnlos sein: „Solange in Düsseldorf eine rote Null als Genosse Finanzministerdarsteller dilettiert, werden seitens des Fiskus die Grundrechte und Rechte der Bürger bestenfalls als unverbindliche Empfehlungen, normalerweise aber als Redaktionsirrtum des Gesetzgebers behandelt.“ Wegen dieser Äußerung verurteilten die Strafgerichte den Beschwerdeführer wegen Beleidigung zu einer Geldstrafe. Der Beschwerdeführer überschreite die Grenze eines Angriffs auf die Ehre des Finanzministers, den er als Person herabwürdige. Zwar werde nicht verkannt, dass die freie Meinungsäußerung ein hohes Rechtsgut sei und dass in der Öffentlichkeit stehende Personen deutliche Kritik auszuhalten hätten. Doch seien auch diese Personen wie andere Bürger geschützt, wenn die Grenze eines persönlichen Angriffs überschritten werde. Auch dies beurteilte die Kammer als Verletzung der Meinungsfreiheit.

Das BVerfG nutzte das Verfahren 1 BvR 2397/19, um seine Rechtsprechung zu Anforderungen des Grundrechts auf Meinungsfreiheit an strafrechtliche Verurteilungen wegen ehrbeeinträchtigender Äußerungen zusammenzufassen.

Art. 5 Abs. 1 Satz 1 GG gibt jedem das Recht, seine Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten, auch wenn dies in polemischer oder verletzender Weise geschieht. Strafrechtliche Verurteilungen wegen Beleidigung (§ 185 StGB) greifen in das Grundrecht der Meinungsfreiheit ein. Die Anwendung dieser Strafnorm erfordert eine der Meinungsfreiheit gerecht werdende Ermittlung des Sinns der infrage stehenden Äußerung und darauf aufbauend im Normalfall eine abwägende Gewichtung der Beeinträchtigungen, die der persönlichen Ehre auf der einen und der Meinungsfreiheit auf der anderen Seite drohen. Hierfür bedarf es einer umfassenden Auseinandersetzung mit den konkreten Umständen des Falles und der Situation, in der die Äußerung fällt. Eine ehrbeeinträchtigende Äußerung ist daher nur dann eine gemäß § 185 StGB tatbestandsmäßige und rechtswidrige (§ 193 StGB) Beleidigung, wenn das Gewicht der persönlichen Ehre in der konkreten Situation die Meinungsfreiheit des Äußernden überwiegt.

Die Kammer zählt wesentliche Abwägungsgesichtspunkte, die je nach der konkreten Situation zu berücksichtigen sind, auf. Maßgeblich ist, dass die konkrete Situation der Äußerung erfasst und unter Berücksichtigung ihrer kontextbezogenen Bedeutung wie ihrer emotionalen Einbettung in Blick auf die betroffenen Grundrechte hinreichend gewürdigt wird. Hierfür kann eine recht knappe Abwägung genügen.

Bei der Abwägung ist mit Blick auf den Inhalt einer Äußerung zunächst deren konkreter ehrschmälernder Gehalt erheblich. Dieser hängt insbesondere davon ab, ob und inwieweit die Äußerung grundlegende, allen Menschen gleichermaßen zukommende Achtungsansprüche betrifft oder ob sie eher das jeweils unterschiedliche soziale Ansehen des Betroffenen schmälert. Das Gewicht der Meinungsfreiheit ist umso höher, je mehr die Äußerung darauf zielt, einen Beitrag zur öffentlichen Meinungsbildung zu leisten, und umso geringer, je mehr es hiervon unabhängig lediglich um die emotionalisierende Verbreitung von Stimmungen gegen einzelne Personen geht. Da der grundrechtliche Schutz gerade aus dem besonderen Schutzbedürfnis der Machtkritik erwachsen ist, ist in die Abwägung gegebenenfalls einzustellen, ob die Privatsphäre des Betroffenen oder sein öffentliches Wirken Gegenstand der Äußerung ist. Dabei kann zwischen Personen zu unterscheiden sein, die wie etwa Politiker bewusst in die Öffentlichkeit treten, und solchen, denen als staatliche Amtswalter ohne ihr besonderes Zutun eine Aufgabe mit Bürgerkontakt übertragen wurde. Der Gesichtspunkt der Machtkritik bleibt allerdings in die Abwägung eingebunden und erlaubt nicht jede auch ins Persönliche gehende Beschimpfung von Amtsträgern oder Politikern. Unzulässig ist eine auf die Person abzielende, insbesondere öffentliche Verächtlichmachung oder Hetze.

Mit Blick auf Form und Begleitumstände einer Äußerung ist erheblich, ob sie unvermittelt in einer hitzigen Situation oder im Gegenteil mit längerem Vorbedacht gefallen ist. Für die Freiheit der Meinungsäußerung wäre es abträglich, wenn vor einer mündlichen Äußerung jedes Wort auf die Waagschale gelegt werden müsste. Erheblich ist zudem, ob und inwieweit für die betreffende Äußerung ein konkreter und nachvollziehbarer Anlass bestand und welche konkrete Verbreitung und Wirkung sie entfaltet. Erhält nur ein kleiner Kreis von Personen von einer ehrbeeinträchtigenden Äußerung Kenntnis oder handelt es sich um eine nicht schriftlich oder anderweitig perpetuierte Äußerung, ist die damit verbundene Beeinträchtigung der persönlichen Ehre geringfügiger und flüchtiger als im gegenteiligen Fall, der je nach Situation bei Äußerungen in „sozialen Netzwerken" im Internet gegeben sein kann. Es ist allerdings nicht allgemein auf das Medium als solches, sondern auf die konkrete Breitenwirkung abzustellen.

Eine solche Abwägung kann entbehrlich sein, wenn herabsetzende Äußerungen die Menschenwürde eines anderen antasten oder sich als Formalbeleidigung oder Schmähung darstellen. Das BVerfG stellte aber klar, dass es sich dabei um Ausnahmefälle handelt, die an strenge Voraussetzungen geknüpft sind. Es genügt nicht die Behauptung, die Voraussetzungen eines Ausnahmetatbestands lägen vor. Die maßgebenden Gründe müssen unter Auseinandersetzung mit den objektiv feststellbaren Umständen des Falles nachvollziehbar dargelegt werden.

Schmähkritik liegt nicht schon bei einem besonderen Gewicht der Ehrbeeinträchtigung vor. Eine Schmähung ist nicht einfach eine besonders drastisch verunglimpfende Form von Beleidigung, sondern bestimmt sich dadurch, dass eine Äußerung keinen irgendwie nachvollziehbaren Bezug mehr zu einer sachlichen Auseinandersetzung hat und es bei ihr allein um das grundlose Verächtlichmachen der betroffenen Person als solcher geht. Es sind dies Fälle, in denen eine vorherige Auseinandersetzung erkennbar nur äußerlich zum Anlass genommen wird, um über andere Personen herzuziehen oder sie niederzumachen, etwa aus verselbständigter persönlicher Feindschaft („Privatfehde") oder aber auch dann, wenn – insbesondere unter den Kommunikationsbedingungen des Internets – Personen ohne jeden nachvollziehbaren Bezug zu einer Sachkritik grundlos aus verwerflichen Motiven wie Hass- oder Wutgefühlen heraus verunglimpft und verächtlich gemacht werden. Davon abzugrenzen sind Fälle, in denen die Äußerung, auch wenn sie gravierend ehrverletzend und damit unsachlich ist, letztlich (überschießendes) Mittel zum Zweck der Kritik oder Ausdruck der Empörung über bestimmte Vorkommnisse ist und damit nicht allein der Verächtlichmachung von Personen dient.

Um eine Formalbeleidigung handelt es sich, wenn mit Vorbedacht und nicht nur in der Hitze einer Auseinandersetzung, nach allgemeiner Auffassung besonders krasse, aus sich heraus herabwürdigende Schimpfwörter – etwa aus der Fäkalsprache – verwendet werden. Bei ihnen ist das maßgebliche Kriterium nicht der fehlende Sachbezug einer Herabsetzung, sondern die kontextunabhängig gesellschaftlich absolut missbilligte und tabuisierte Begrifflichkeit, die die Betroffenen insgesamt verächtlich macht, und damit die spezifische Form dieser Äußerung.

Die Meinungsfreiheit muss zudem stets zurücktreten, wenn eine Äußerung die Menschenwürde eines anderen verletzt. Dies kommt nur in Betracht, wenn sich die Äußerung nicht lediglich gegen einzelne Persönlichkeitsrechte richtet, sondern einer konkreten Person den ihre menschliche Würde ausmachenden Kern der Persönlichkeit abspricht (BVerfG, PM Nr. 49/2020 v. 19.06.2020, Klarstellung verfassungsrechtlicher Maßgaben für strafrechtliche Verurteilungen wegen ehrbeeinträchtigender Äußerungen).

### BVerfG

## Beschränktes „Recht auf Vergessenwerden" bei Promis

Das Bundesverfassungsgericht (BVerfG) stellte in einem Beschluss vom 23.06.2020 fest, dass ein Prominenter, der vor 40 Jahren an der Uni schummelte, auch heute noch Berichte darüber aushalten muss, und bekräftigte damit die Pressefreiheit bei der Berichterstattung über weit zurückliegende Fehltritte bekannter Persönlichkeiten (Az. 1 BvR 1240/14). Die Möglichkeit, Dinge zu erwähnen, die der Betroffene ungern über sich in der Zeitung liest, erlösche

nicht „schematisch durch bloßen Zeitablauf". Demzufolge kann die Presse selbst beurteilen, welche Umstände sie für erheblich hält – auch in Zeiten des Internets. Maßgeblich seien das Berichterstattungsinteresse und dass es für die Erwähnung „objektivierbare Anknüpfungspunkte" gibt.

Geklagt hatte ein Wirtschaftsmagazin. Darin war 2011 ein mehrseitiges Porträt über einen Unternehmer erschienen, der damals als Vorstandsvorsitzender ein börsennotiertes Krankenhausunternehmen leitete. In dem Beitrag wurde geschildert, dass der Firmenchef und frühere Spitzenkandidat der rechtskonservativen Schillpartei Jura studiert hatte und wegen eines Täuschungsversuchs 1983 vom Staatsexamen ausgeschlossen wurde. Gegen den Bericht hatte der Mann erfolgreich geklagt. Die Gerichte in Hamburg argumentierten damals, er dürfe nicht dauerhaft an den Pranger gestellt werden.

Das BVerfG entschied nun, dass diese Gerichtsentscheidungen verkennen, dass der Unternehmer öffentlich tätig war und selbst die Öffentlichkeit suchte. Eine Person wie er könne „nicht verlangen, dass ihre in der Vergangenheit liegenden Fehler, nicht aber ihre Vorzüge, in Vergessenheit geraten". Die Gefahr, ausgegrenzt zu werden, bestehe nicht. Der Täuschungsversuch sei „kein Makel, der geeignet wäre, das Gesamtbild einer Person zu dominieren und ein selbstbestimmtes Privatleben des Betroffenen ernstlich zu gefährden".

Der Beschluss weist aber auch darauf hin, dass es andere Fälle geben kann: Menschen, die dazu keinen Anlass gäben, müssten es nicht unbegrenzt hinnehmen, „in aller Öffentlichkeit mit ihrem gesamten, teils lange zurückliegenden Verhalten förmlich zermürbt zu werden". Grenzen der Berichterstattung liegen vor, wenn der Kern der Privatsphäre betroffen ist, etwa bei Ausführungen zur sexuellen Orientierung. Unzulässig ist es demnach, wenn die Berichterstattung den Betroffenen wegen seines lang zurückliegenden Verhaltens „förmlich zermürbt". Dies sei hier nicht der Fall gewesen. Das Landgericht Hamburg muss nun noch einmal über die Klage des Mannes entscheiden und die Vorgaben aus Karlsruhe berücksichtigen (Prominente müssen sich Berichte über frühere Fehltritte gefallen lassen, www.spiegel.de 09.07.2020; Vergangene Fehler, SZ 10.07.2020, 27).

### BVerfG

## Journalistischer Persönlichkeitsschutz erst bei Foto-Publikation

Das Bundesverfassungsgericht (BVerfG) hat mit Beschluss vom 23.06.2020 die strafrechtliche Verurteilung eines Fotojournalisten wegen Verletzung der Pressefreiheit aufgehoben, der in einer Krankenhausnotaufnahme entgegen dem Wunsch der Betroffenen Fotos machte, wovon eines später unverpixelt im Internet unter bild.de veröffentlicht worden war (Az. 1 BvR 1716/17).

Es war im Oktober 2014, als der Fotograf das Wort „Ebola" an der Anmeldung der Notaufnahme des Krankenhauses aus dem Gespräch zwischen einem Mann und Klinikmitarbeitern aufschnappte und dann weiter die Worte Kongo, Belgien und Fieber. Er wurde aufgefordert, bitte Abstand zu halten und man händigte ihm Mundschutz und Handschuhe aus. Für einen Fotografen, der gerade an einer Dokumentation über die sich damals verbreitende Epidemie arbeitete, genügten die Wortfetzen, um auf den Auslöser zu drücken: ein Ebola-Verdachtsfall im offenen Wartebereich, wo 40 Patienten warteten. Das Foto landete auf Bild.de unter der Schlagzeile „Ebola Panne in NRW? Virus-Verdächtiger musste auf Klinik-Flur warten." Auf dem Foto war der dunkelhäutige Patient deutlich erkennbar. Dem Fotografen trug das unverpixelt bei Bild.de veröffentlichte Foto eine Geldstrafe in Höhe von 3200 Euro (40 Tagessätze) wegen unbefugter Weitergabe von Bildaufnahmen ein. Der Mann hatte sich die Fotos noch auf dem Klinikflur verbeten, die behandelnde Ärztin verlangte deren Löschung und informierte den Fotografen, dass sich der Ebola-Verdacht nicht bestätigt habe.

Die Aufhebung der Verurteilung begründete das BVerfG wie folgt: Ob ein Foto zum Schutz der Betroffenen verpixelt werden muss oder nicht, das habe die Redaktion vor der Veröffentlichung zu entscheiden und nicht bereits der Fotograf, bevor er die Aufnahmen überhaupt anbietet. Das bloße Anfertigen der Bilder und die anschließende Weitergabe an die Zeitung dient danach der Vorbereitung einer Veröffentlichung und ist geschützt von der Pressefreiheit: „Es liegt jedenfalls in der Regel in der Verantwortung der jeweiligen Redaktionen, bei einer Veröffentlichung von Bildaufnahmen die Rechte der Abgebildeten zu wahren".

Zwar spricht, so das BVerfG im konkreten Fall, viel dafür, dass das Gesicht des Patienten hätte verpixelt werden müssen, trotz des großen öffentlichen Interesses, auf das sich die Zeitung für Berichte über unzureichende Sicherheitsvorkehrungen in einer Klinik berufen konnte. Ein solches Foto bedeute eine erhebliche Stigmatisierung und öffentliche Bloßstellung des Mannes, womit das Landgericht Köln die strafrechtliche Verurteilung begründet hatte. Laut BVerfG muss der Fotograf den Kollegen in der Redaktion nicht die Entscheidung darüber abnehmen, was gezeigt werden darf und was nicht.

Damit seien aber die Fotografen nicht bloße Diener ihrer Herren in der Redaktion. Der Kontext, in dem eine Aufnahme gemacht wurde, kann für die Frage entscheidend sein, ob und in welcher Form ein Bild gedruckt oder veröffentlicht werden darf. Im konkreten Fall war es nicht ganz eindeutig, wie präzise der Fotograf die Redaktion über die Situation im Klinikflur informiert hatte; jedenfalls hatten mehrere Nachrichtenagenturen zuvor das Foto dankend abgelehnt. Über Verpixelung wurde mit Bild.de nicht gesprochen, soviel ist klar. Aber das BVerfG unterstellte, dass er die Redaktion ordnungsgemäß über den Widerspruch des Betroffenen und den Protest der Ärztin in Kenntnis gesetzt habe; dass dies verschwiegen worden wäre, sei jedenfalls nicht gerichtlich festgestellt worden (Janisch, Die Pflicht zum Pixeln liegt bei der Redaktion, www.sueddeutsche.de 08.07.2020 = SZ 09.07.2020, 15).

### BVerfG

## § 113 Telekommunikationsgesetz verfassungswidrig

Das Bundesverfassungsgericht (BVerfG) in Karlsruhe stellte in einem Beschluss

vom 27.05.2020 fest, dass der aktuell praktizierte Abruf von den bei Telekommunikationsunternehmen gespeicherten Bestands- und Abrechnungsdaten sowie PIN-Nummern durch Strafverfolger und Nachrichtendienste gegen die informationelle Selbstbestimmung und das allgemeine Persönlichkeitsrecht verstößt (1 BvR 1873/13, 1 BvR 2618/13). § 113 des Telekommunikationsgesetzes (TKG) und mehrere Fachgesetze des Bundes, die die Bestandsdatenauskunft regeln, wurden für verfassungswidrig erklärt: „Sie verletzen die Beschwerde führenden Inhaber von Telefon- und Internetanschlüssen in ihren Grundrechten auf informationelle Selbstbestimmung sowie auf Wahrung des Telekommunikationsgeheimnisses."

Die Beschwerde des Piraten-Politikers Patrick Breyer und seiner ehemaligen Kollegin Katharina Nocun hatte sich gegen eine 2013 auf Druck des Verfassungsgerichts schon einmal nachgebesserte Regelung gerichtet. Die Entscheidung der Karlsruher Richter stellt zugleich die gerade erst verabschiedete Regelung zur Bestandsdatenauskunft im Gesetz gegen Hasskriminalität in Frage. Breyer unterstrich, dass der Zugriff des Staates auf Kommunikationsdaten mit richterlicher Anordnung und zur Aufklärung schwerer Straftaten oder zur Abwehr von Gefahren für wichtige Rechtsgüter unbestritten sei, gerade auch vor dem Hintergrund des härter gewordenen Tons im Netz: „Das Gesetz zur Bestandsdatenauskunft geht aber weit darüber hinaus. Es erfasst schon Ordnungswidrigkeiten, gilt für Geheimdienste, betrifft Personen, die keinerlei Straftat verdächtig sind."

So sah es nun auch der erste Senat des BVerfG. Die Erteilung einer Auskunft über Bestandsdaten sei grundsätzlich verfassungsrechtlich zulässig. Der Gesetzgeber müsse aber „sowohl für die Übermittlung der Bestandsdaten durch die Telekommunikationsanbieter als auch für den Abruf dieser Daten durch die Behörden jeweils verhältnismäßige Rechtsgrundlagen schaffen." Übermittlungs- und Abrufregelungen müssten die Verwendungszwecke der Daten hinreichend begrenzen und dabei die Tiefe des Eingriffs in die Privatsphäre an den jeweiligen Tatbestand anpassen. Auch die Möglichkeit für die Betroffenen, sich gerichtlich gegen die Maßnahmen zu wehren, muss ausbalanciert sein. „Die genannten Voraussetzungen wurden von den angegriffenen Vorschriften weitgehend nicht erfüllt." Im Übrigen habe man „wiederholend festgestellt, dass eine Auskunft über Zugangsdaten nur dann erteilt werden darf, wenn die gesetzlichen Voraussetzungen für ihre Nutzung gegeben sind."

Mit den jetzt für verfassungswidrig erklärten Bestimmungen im TKG fallen auch die korrespondierenden Abrufregelungen im Bundeskriminalamtsgesetz (BKAG), im Bundespolizeigesetz, im Zollfahndungsdienstgesetz, im Bundesverfassungsschutzgesetz, im BND-Gesetz und im MAD-Gesetz. Diese „genügen weitgehend ebenfalls nicht den verfassungsrechtlichen Anforderungen".

Das BVerfG räumte ein, dass die Abrufregelungen einigermaßen bestimmte und normenklare spezifische Ermächtigungsgrundlagen geschaffen haben. Mit Blick auf ihr Eingriffsgewicht sei die Verhältnismäßigkeit aber „überwiegend" nicht gewahrt. Beispielsweise müssten „Abrufregelungen, die zum Abruf von Bestandsdaten anhand dynamischer IP-Adressen ermächtigen, neben einer hinreichenden Begrenzung der Verwendungszwecke auch eine nachvollziehbare und überprüfbare Dokumentation der Entscheidungsgrundlagen des Abrufs vorsehen". Dies war im Gesetz nicht vorgesehen.

Das BVerfG betonte, dass es gerade mit Blick auf den nachrichtendienstlichen Zugriff, beziehungsweise den Zugriff für die Gefahrenabwehr, „grundsätzlich einer im Einzelfall vorliegenden konkreten Gefahr und für die Strafverfolgung eines Anfangsverdachts" bedarf. Breyer und Nocun hatten in ihrer Beschwerde gewarnt, dass nicht zuletzt durch die Auflagen für Telekommunikationsprovider, eine technische Schnittstelle vorzuhalten, zu einem massenhaften Abruf ermuntert werde. In diesem Argument sahen sich die Bürgerrechtler auch durch die Stellungnahme der damaligen Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI), Andrea Voßhoff, und anderer Datenschützer bestätigt.

Voßhoff hatte gemahnt, dass das Auskunftsrecht der Behörden praktisch unbeschränkt sei. Auch der nach und nach bekannt gewordene Anstieg manueller Abfragen durch das BKA von gut 2000 Anfragen 2013 auf 17.428 Anfragen 2017 mit weiterhin steigender Tendenz und einer hohen Dunkelziffer bestätigte die Sorgen der Beschwerdeführer.

Die Entscheidung ist aus Sicht der Beschwerdeführer hochrelevant für das jüngst beschlossene Gesetz zur „Hasskriminalität", das den staatlichen Datenzugriff auf Internetunternehmen wie Facebook, Google oder Twitter erweitert. Breyer: „Mit dem ‚Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität' wird die Bestandsdatenauskunft auf Telemediendienste sogar noch erweitert (s. u.a. §§ 15a, 15b TKG). Sogar Internet-Passwörter sind zu beauskunften." Leider komme das Urteil nun zu spät, um noch im aktuellen Gesetzgebungsverfahren berücksichtigt zu werden. „Wir müssen daher möglicherweise erst jahrelang erneut aufwendig Verfassungsbeschwerde erheben." Er habe das Bundesverfassungsgericht gebeten, vor Beschluss dieses Gesetzes zu entscheiden, aber ohne Erfolg. Angesichts der vielen Klagen, die der Gesetzgeber besorgten Bürgern und Politiker in den vergangenen Jahren aufgebürdet hat, konstatiert er einen Konstruktionsfehler im gesetzgeberischen System. Grundrechtswidrige Überwachungsgesetze für „sicherheitsfanatische Politiker ‚lohnten' (sich), weil sie schlimmsten- oder bestenfalls Jahre später zurückgestutzt würden, jeweils noch mit Übergangszeit. Die Politik betreibt vorsätzlichen Verfassungsbruch."

Den Piraten schweben zur Verhinderung verfassungswidriger Gesetze mehrere neue Mechanismen vor. So sollen ein Drittel des Deutschen Bundestages oder zwei Fraktionen das Recht erhalten, ein Rechtsgutachten des Bundesverfassungsgerichts zur Verfassungskonformität eines Gesetzesvorhabens einzuholen. Außerdem soll der Bundespräsident bei verfassungsrechtlichen Zweifeln vor der Ausfertigung eines Gesetzes das Bundesverfassungsgericht anrufen können. Schließlich sollen nach dem Vorbild anderer Verbandsklagerechte auch Bürgerrechtsorganisationen die Möglichkeit bekommen, stellvertretend für die Allgemeinheit vor den Fachgerichten und dem Bundesverfas-

sungsgericht gegen Grundrechtsverletzungen zu klagen.

Das Telekommunikationsgesetz und entsprechende Vorschriften in anderen Gesetzen müssen nun bis spätestens Ende 2021 überarbeitet werden. Solange bleiben die beanstandeten Regelungen unter bestimmten Maßregeln in Kraft (Ermert, Verfassungsgericht: Staatlicher Zugriff auf Bestandsdaten muss begrenzt werden, www.heise.de 17.07.2020, Kurzlink: https://heise.de/-4846316).

**BGH**

## EuGH soll Verbandsklagebefugnis nach DSGVO klären

Der Bundesgerichtshof (BGH) legte mit Beschluss von 28.05.2020 dem Europäischen Gerichtshof (EuGH) die Frage vor, ob ein Verbraucherverband, hier der Verbraucherzentrale Bundesverband (vzbv), ohne Auftrag von Betroffenen gegen Datenschutzverstöße gerichtlich vorgehen darf (Az. I ZR 186/17). Im Ausgangsverfahren geht es um ein sogenanntes App-Zentrum von Facebook, in dem Nutzer kostenlos auf Online-Spiele anderer Anbieter zugreifen können. Im November 2012 wurden hier mehrere Spiele angeboten, bei denen unter dem Button „Sofort spielen" folgende Hinweise zu lesen waren: „Durch das Anklicken von ‚Spiel spielen' oben erhält diese Anwendung: Deine allgemeinen Informationen, Deine-Mail-Adresse, Über Dich, Deine Statusmeldungen. Diese Anwendung darf in deinem Namen posten, einschließlich deinen Punktestand und mehr." Bei einem Spiel endeten die Hinweise mit dem Satz: „Diese Anwendung darf Statusmeldungen, Fotos und mehr in deinem Namen posten." Dagegen klagte der vzbv und beanstandete die gegebenen Hinweise als unlauter unter anderem unter dem Gesichtspunkt des Rechtsbruchs wegen der fehlenden Einholung einer wirksamen datenschutzrechtlichen Einwilligung des Nutzers. Ferner sah er in dem abschließenden Hinweis bei einem Spiel eine den Spieler unangemessen benachteiligende allgemeine Geschäftsbedingung.

Das angerufene Landgericht Berlin hat Facebook deswegen antragsgemäß verurteilt (U.v. 28.10.2014 – 16 O 60/13). Das soziale Netzwerk soll es unterlassen Spiele so zu präsentieren, dass Nutzer mit dem Betätigen eines Buttons dem Spieleanbieter erlauben, personenbezogene Daten in ihrem Namen zu posten. Die Berufung der Beklagten beim Kammergericht Berlin hatte keinen Erfolg (U. v. 22.09.2017 – 5 U 155/14). Mit ihrer vom Berufungsgericht zugelassenen Revision verfolgt Facebook den Antrag auf Klageabweisung jedoch weiter.

Der BGH hat die Sache nun an den EuGH zur Vorabentscheidung vorgelegt. Der soll klären, ob die getroffenen Bestimmungen nationalen Regelungen entgegenstehen oder nicht. Ob Mitbewerber, Verbände und andere Institutionen wegen Verstößen gegen die Datenschutz-Grundverordnung (DSGVO) unabhängig von der Verletzung konkreter Rechte einzelner betroffener Personen und ohne Auftrag einer betroffenen Person gegen den Verletzer vor Zivilgerichten vorgehen dürfen, ist bei Fachleuten und in der Rechtsliteratur umstritten und bedarf einer verbindlichen Feststellung. Der EuGH hat zwar schon entschieden, dass die Regelungen der – bis zum Inkrafttreten der DSGVO am 25.05.2018 geltenden – Richtlinie 95/46/EG (Datenschutzrichtlinie) einer Klagebefugnis von Verbänden nicht entgegenstehen (U. v. 29.07.2019 – C-40/17). Dieser Entscheidung ist allerdings nicht zu entnehmen, ob diese Klagebefugnis unter Geltung der an die Stelle der Datenschutzrichtlinie getretenen Datenschutz-Grundverordnung fortbesteht (Dierks, EuGH soll klären, ob Verbraucherschützer klagen dürfen, www.heise.de 28.05.2020, Kurzlink: https://heise.de/-4768144).

**BGH**

## Facebook missbraucht Marktmacht beim Zusammenführen von Nutzerdaten

Der Bundesgerichtshof (BGH) hat mit Beschluss vom 23.06.2020 eine Verbotsverfügung des Bundeskartellamtes (BKartA) in Bonn formell bestätigt, dass der Konzern seine marktbeherrschende Stellung ausgenutzt hat, um die Nutzer zur Preisgabe ihrer Nutzungsdaten zu bewegen und verpflichtet ist, die Zusammenführung von Nutzerdaten zu stoppen (Az. KVR 69/19). Das Bundeskartellamt hatte Anfang 2019 dem US-Konzern aufgegeben, das Zusammenführung von Nutzerdaten aus den unterschiedlichen Diensten wie WhatsApp und Instagram und das Sammeln von Nutzerdaten auf fremden Websites etwa mit dem „Gefällt-mir"-Button (sog. Off-Facebook-Daten) einzustellen (DANA 2/2019, 84 f.). Insbesondere die Übernahme von WhatsApp durch Facebook war den Kartellwächtern ein Dorn im Auge, mit der sich der Konzern eine unangefochtene Vormachtstellung auf dem Markt für Instant-Messenger sicherte.

Das Oberlandesgericht Düsseldorf (OLG) hatte jedoch mit Beschluss vom 26.08.2019 den Vollzug der Entscheidung außer Kraft gesetzt, da die Richter Zweifel hatten, ob die Verfügung rechtlich Bestand haben könnte (DANA 4/2019, 239 f.). Mit dem Beschluss des BGH wurde dieser Stopp wieder aufgehoben: Nur wenn die Nutzer explizit zustimmen, darf Facebook weiterhin Daten zusammenführen. Der BGH hat nach seiner vorläufigen Bewertung „keine ernstlichen Zweifel", dass Facebook seine marktbeherrschende Stellung missbraucht hat. Bei der rechtlichen Bewertung spielen vor allem zwei Aspekte eine Rolle: Zum einen hatte sich das BKartA bei seiner Entscheidung sehr ausführlich auf Verstöße gegen die Datenschutz-Grundverordnung gestützt, obwohl die Bonner Behörde in diesem Bereich keine direkte Zuständigkeit hat. Das OLG stellte infrage, ob das Abfordern von Daten der Endnutzer mit einer missbräuchlichen Preissetzung zu vergleichen sei, gegen die die Kartellwächter vorgehen können.

Zum anderen stellt sich die Frage, nach welchen Maßstäben eine marktbeherrschende Stellung im Social-Media-Markt gemessen werden sollte. Facebook verweist auf einen gesunden Wettbewerb mit Apps wie YouTube, Twitter und Snapchat, während das BKartA auf die Nutzungszahlen der von Facebook betriebenen Angebote verwies. Hier sei Facebook weit vor der Konkurrenz.

In beiden Punkten stellten sich die Karlsruher Richter hinter die Bonner Behörde, legten aber deutlich andere Begründungen zugrunde: „Es bestehen weder ernsthafte Zweifel an der marktbeherrschenden Stellung von Facebook auf dem deutschen Markt für soziale Netzwerke noch daran, dass Facebook diese marktbeherrschende Stellung mit den vom Kartellamt untersagten Nutzungsbedingungen missbräuchlich ausnutzt." Ein Verstoß gegen die Datenschutz-Grundverordnung stehe hierbei aber nicht im Vordergrund. Entscheidend sei vielmehr, dass den privaten Facebook-Nutzern keine Wahlmöglichkeit gelassen werde, auf welche Daten der Konzern konkret zugreifen kann: „Facebook muss den Nutzern die Möglichkeit geben, weniger von sich preiszugeben." So können Nutzer der Übernahme von Daten aus Dritt-Quellen nicht wirksam widersprechen, wenn sie den Geschäftsbedingungen von Facebook insgesamt zustimmen.

Zwar kann Facebook dank der Ende-zu-Ende-Verschlüsselung die Nachrichten zwischen WhatsApp-Nutzern nicht direkt mitlesen. Die Datenschutzerklärung gibt Facebook allerdings freie Bahn, alle begleitenden Daten auszuwerten – von der verwendeten Telefonnummer über die Facebook-ID parallel installierter Apps bis hin zum Akkuladezustand eines Smartphones. Diese Daten werden laut WhatsApp auch mit Daten Dritter kombiniert und zum Marketing verwendet. Auch über auf Dritt-Websites eingebettete Facebook-Pixel und PlugIns in Apps sammelt Facebook viele Nutzungsdaten, um sie zur Werbevermarktung zu nutzen.

Angesichts der enormen Datenfülle könne der Nutzer nicht mehr das Recht auf informelle Selbstbestimmung wahrnehmen. Der BGH verweist auf den „Lockin-Effekt": Zwar können sich die Nutzer problemlos auch bei anderen sozialen Netzwerken anmelden. Wenn sie mit ihrem Kontaktnetzwerk auf Kanälen außerhalb von Facebook in Verbindung bleiben wollen, ist dies jedoch mit enormem Aufwand verbunden, wenn nicht gar unmöglich, da man jeden Kontakt überreden muss, sich beim gleichen Konkurrenten anzumelden.

Gäbe es tatsächlich einen funktionierenden Wettbewerb, sei zu erwarten, dass es auch datenschonendere Angebote gebe. Die Endnutzer haben nach Überzeugung des Gerichts hier klare Prioritäten. Diese wahrzunehmen sei aber kaum möglich, wenn Facebook dank seiner Marktmacht einen enormen Informationsvorsprung aufgebaut habe und so ein für Nutzer wesentlich attraktiveres Angebot aufbauen könne. Zudem könne Facebook dank seiner Größe viel höhere Werbeerträge erzielen als potenzielle Konkurrenten. Alles in allem diagnostizieren die Richter somit einen Missbrauch der marktbeherrschenden Stellung.

Der Kartellsenat des BGH hat mit seinem Beschluss eine grundlegende Weichenstellung vorgenommen. So könnte das Geschäftsgebaren von Facebook auch eingeschränkt werden, wenn keine marktbeherrschende Stellung auf dem Werbemarkt für soziale Netzwerke nachgewiesen sei: „Die Beeinträchtigung muss nicht auf dem beherrschten Markt eintreten, sondern kann auch auf einem nicht beherrschten Drittmarkt eintreten." Zwar handelt es sich bei dem BGH-Beschluss nur um eine vorläufige Eilentscheidung, doch hat sich das Gericht bei einigen zentralen Fragen klar festgelegt. Die Daten, die ein Nutzer hergibt, sind nicht allein schützensbedürftige Informationen, sondern Eintrittspreis für die schöne bunte Netzwerkwelt. Facebook-Anwalt Thomas Winter hatte vorgetragen, es könne ja wohl nicht sein, dass Facebook gezwungen werde, den Kunden anstatt des besten Produkts eine schlechtere Leistung anzubieten. Dem hielt der BGH-Senatsvorsitzende Peter Meier-Eck entgegen, es könne nicht richtig sein, dass ein marktbeherrschender Akteur bei der Entwicklung seiner Angebote keinen Schranken unterliege. Facebook sei „ubiquitär". Der Vertreter des BKartA Jörg Nothdurft hatte zuvor gemeint: „Dass man mit seinem gesamten Surfverhalten bezahlt, um Facebook zu nutzen, ist kartell- und datenschutzrechtlich nicht hinnehmbar" (Kleinz, BGH: Bundeskartellamt darf Facebooks Datensammlung stoppen, www.heise.de 23.06.2020; Kurzlink: https://heise.de/-4793293; Janisch, Bundeskartellamt gegen Facebook, SZ 24.06.2020, 18).

**BGH**

## Werbe-Cookies nur mit ausdrücklicher Einwilligung

Der Bundesgerichtshof (BGH) hat mit Urteil vom 28.05.2020 auf die Klage des Verbraucherzentrale Bundesverbands (vzbv) gegen Planet49 entschieden, dass Website-Betreiber die Zustimmung zur Speicherung der Cookies von Drittanbietern nicht einfach voraussetzen dürfen (Az. I ZR 7/16). Konkret ging es um zwei Sachverhalte: Zum einen hatte Planet49 die „Zustimmung" zu Cookies eingeholt, indem den Nutzern ein vorausgewähltes Ankreuzfeld präsentiert wurde. Wählten die Nutzer das Feld nicht explizit ab, ging der Anbieter von einer erteilten Zustimmung aus. Zudem wurde von den Gewinnspielteilnehmern weitgehende Zustimmung zu invasiven Werbemaßnahmen wie Werbeanrufen abverlangt.

In beiden Fällen entschieden die Karlsruher Richter im Sinne der klagenden Verbraucherschützer. Sowohl zur telefonischen Werbung als auch zum Weiterreichen einer Cookie-ID an Drittunternehmen fehle es an einer wirksamen Einwilligung der Verbraucher. Eine solche liege erst vor „wenn der Verbraucher weiß, dass seine Erklärung ein Einverständnis darstellt und worauf sie sich bezieht". Zwar konnten die Gewinnspielteilnehmer in einem Dialog aussuchen, mit welchen Sponsoren sie Daten teilen wollten – diese Informationen waren jedoch erst nach weiteren Klicks ersichtlich.

Deutschland hatte in Sachen Cookies einen Sonderweg eingeschlagen, indem es im Telemediengesetz (TMG) die Vorgaben aus dem europäischen Recht nicht vollständig umgesetzt hat. Dies führte dazu, dass viele deutsche Anbieter ihren Kunden lediglich ermöglichten, der Speicherung der Cookies per Opt-out zu widersprechen. Wenn die entsprechenden Cookie-Warnungen ignoriert wurden, galt die Zustimmung als erteilt. Nach Inkrafttreten der europäischen Datenschutz-Grundverordnung (DSGVO) wurde dieser Widerspruch immer offensichtlicher. Um die eigene Interpretation abzusichern, hatte der Bundesgerichtshof mit mehreren Fragen den Europäischen Gerichtshof

(EuGH) angerufen, um die europarechtliche Dimension des Falls zu klären. Der EuGH entschied im Oktober 2019, dass es einer ausdrücklichen Zustimmung nach einer detaillierten Information bedarf, um Werbe-Cookies von Dritten speichern zu dürfen. Ob das deutsche Recht jedoch den EU-Vorgaben widerspricht, stellten die Luxemburger Richter nicht explizit fest (DANA 4/2019, 234).

Auch der BGH stellte keinen expliziten Gegensatz zwischen der europäischen und deutschen Gesetzeslage fest. So sei das Vorgehen des Gewinnspielanbieters bereits nach der Rechtslage von vor 2018 unzulässig gewesen, da es „mit wesentlichen Grundgedanken des § 15 Abs. 3 Satz 1 TMG unvereinbar" gewesen sei. Dass dem deutschen Gesetz entsprechende Umsetzungsvorschriften zu den EU-Richtlinien fehlten, sei hier nicht entscheidend, „denn es ist anzunehmen, dass der Gesetzgeber die bestehende Rechtslage in Deutschland für richtlinienkonform erachtete." Der Wortlaut der Vorschrift lasse eine dementsprechende Interpretation zu, die die Richter nun anwendeten. Gehe man von der inzwischen überarbeiteten Rechtslage aus, komme man zum gleichen Ergebnis.

Das Urteil hat grundsätzliche Bedeutung: Bereits im Vorfeld der Entscheidung haben viele deutsche Website-Betreiber ihre Cookie-Warnungen umgestellt, sodass Nutzer explizit der Datenverarbeitung zustimmen müssen. Die Konferenz der deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder hatte schon mehr als zwei Jahre zuvor klargestellt, dass die Berufung auf das Telemediengesetz unzulässig ist. Seit über einem Jahr fanden intensive Gespräche der Datenschutzaufsicht statt mit Branchen, die mit ihren Bannern gegen das Gesetz verstoßen. Bußgelder wurden aber bisher keine verhängt, was ein Landesdatenschützer erklärt: „Mit Sanktionen würden wir eher gegen schwarze Schafe als gegen Branchen vorgehen. Und bei Cookies sind ganze Branchen, die man gemeinhin für seriös hält, auf einem schwierigen Trip." Dennoch zeigte sich der Branchenverband Bitkom wenig begeistert von der BGH-Entscheidung. Geschäftsführer Bernhard Rohleder meinte, dass das Urteil Webseitenbetreiber schwer treffe und viele Internetnutzer nerve. Neben den hohen Auflagen der DSGVO müssten die Betreiber von Webseiten jetzt zusätzliche Prozesse und Formulare für ihre Webangebote einführen, um Cookies auch künftig nutzen zu dürfen.

Parallel dazu haben Gegenmaßnahmen von Browserherstellern wie Apple dazu geführt, dass der Gebrauch von Third-Party-Cookies weiter zurückgedrängt wird. Die Bundesregierung hat im Herbst 2019 eine Neufassung des Telemediengesetzes angekündigt, die nach dem Richterspruch aus Karlsruhe nun auf den Weg gebracht werden kann (Kleinz, Bundesgerichtshof: Cookies nur mit aktiver Einwilligung, www.heise.de 28.05.2020, Kurzlink: https://heise.de/-4767977; Hauck/Muth, Die Sache mit dem Haken, SZ 29.05.2020, 17).

### VG Wiesbaden

## Fluggastdatengesetz auf dem EuGH-Prüfstand

Mit Beschlüssen vom 13. und 15.05.2020 hat die 6. Kammer des Verwaltungsgerichts Wiesbaden (VG) im Rahmen von Vorabentscheidungsersuchen dem Europäischen Gerichtshof (EuGH) Fragen betreffend das Fluggastdatengesetz vorgelegt (6 K 805/19.WI u. 6 K 806/19.WI). In beiden Verfahren begehren die Kläger die Löschung ihrer sog. Fluggastdaten (PNR-Daten, Passenger Name Record), die vom Bundeskriminalamt (BKA) gespeichert werden. Das Verfahren 6 K 805/19.WI betrifft dabei Flüge aus der Europäischen Union (EU) in einen Drittstaat, das Verfahren 6 K 806/19.WI betrifft Flüge innerhalb der EU.

Am 27.04.2016 hatten das Europäische Parlament und der Rat die Richtlinie (EU) 2016/681, die sog. PNR-Richtlinie, erlassen. Diese schreibt vor, dass die Fluggesellschaften bei sämtlichen Flügen von der Union in Drittstaaten und von Drittstaaten in die Union eine Vielzahl von personenbezogenen Daten aller Fluggäste an von den jeweiligen Mitgliedstaaten einzurichtende Zentralstellen (in Deutschland: das Bundeskriminalamt) übermitteln müssen, wo diese Daten automatisiert mit Datenbanken und Algorithmen (sog. Mustern) abgeglichen und fünf Jahre lang gespeichert werden. Auch eine Weitergabe an andere Behörden im In- und Ausland ist gestattet. Diese Maßnahmen sollen der Bekämpfung von Terrorismus und schwerer Kriminalität dienen. Die Bundesrepublik Deutschland hat, ebenso wie viele andere EU-Mitgliedstaaten, mit Erlass des Fluggastdatengesetzes vom 06.06.2017 die Richtlinie umgesetzt und von der durch die Richtlinie explizit eröffneten Möglichkeit Gebrauch gemacht, die Fluggastdatenverarbeitung auch auf alle innereuropäischen Flüge auszuweiten.

Die durch das VG Wiesbaden nun dem Europäischen Gerichtshof zur Beantwortung vorgelegten Fragen betreffen im Wesentlichen die Vereinbarkeit der PNR-Richtlinie und des Fluggastdatengesetzes mit der Charta der Grundrechte der Europäischen Union (GRCh), insbesondere den dort verankerten Grundrechten auf Achtung des Privat- und Familienlebens (Art. 7 GRCh) und dem Schutz personenbezogener Daten (Art. 8 GRCh) sowie mit der Datenschutz-Grundverordnung und (im Falle der innereuropäischen Flüge) mit der durch den AEUV (Vertrag über die Arbeitsweise der Europäischen Union) innerhalb der Europäischen Union garantierten Freizügigkeit (Art. 21 AEUV).

Das Gericht äußert erhebliche Zweifel, ob die PNR-Richtlinie und das deutsche Umsetzungsgesetz europarechtskonform sind. Es hält die Fluggastdatenverarbeitung mit der Vorratsdatenspeicherung von Telekommunikationsdaten für vergleichbar und erachtet die damit verbundenen Grundrechtseingriffe trotz des verfolgten Ziels (Bekämpfung von Terrorismus und schwerer Kriminalität) als nicht gerechtfertigt. Zweifelhaft seien demnach unter anderem der Umfang der erhobenen und verarbeiteten Fluggastdaten, die Verhältnismäßigkeit der 5-jährigen Speicherdauer für die Fluggastdaten, die Bestimmtheit mehrerer Vorschriften der Richtlinie und des Umsetzungsgesetzes, ob die Fluggäste über die Datenverarbeitung ausreichend informiert werden, ob die Weitergabe an Drittstaaten und inländisch an das Bundesamt für Verfassungsschutz zu-

lässig ist und ob die Mehrfacherfassung der Fluggäste (durch Start- und Zielland des jeweiligen innereuropäischen Fluges) gerechtfertigt ist. Die Verfahren des VG Wiesbaden werden dann nach der EuGH-Entscheidung über die Vorabentscheidungsersuchen fortgesetzt (Verwaltungsgericht Wiesbaden: Vorschriften des Fluggastdatengesetzes auf dem Prüfstand, Presseinformation v. 19.05.2020).

**LG Tübingen**

## Polizeiliche Wohnprojekte-Videoüberwachung war unzulässig

Das Landgericht Tübingen (LG) hat mit Beschluss vom 11.03.2020 den Strafverfolgungsbehörden, also Polizei und Staatsanwaltschaft, untersagt, zwei linke Wohnprojekte in Tübingen einer Langzeit-Videoüberwachung zu unterziehen (Az. 9 Qs 28/20). Das LG erklärte die im Jahre 2016 für zwei Monate angeordnete allnächtliche Videoüberwachung der Wohnprojekte für rechtswidrig und hob eine gegenteilige Entscheidung des Amtsgerichts Tübingen auf.

Die Videoüberwachung war angeordnet worden, weil es sich bei diesen Wohnprojekten „um einschlägig bekannte linke Szeneobjekte (gehandelt habe), in welchen Angehörige der linksautonomen Szene wohnhaft sind". In „fußläufiger Nähe" seien vier PKWs Gegenstand von Brandstiftungen geworden. Nachträgliche Bekennerschreiben in der zwischenzeitlich verbotenen Plattform „linksunten.indymedia.org" und ein erst nach dem Löscheinsatz am nächsten Tage festgestelltes Graffiti „R94" ließen die Polizei von sog. Resonanzstraftaten auf die Räumung des besetzten Hauses Rigaer Str. 94 in Berlin ausgehen. Wegen Erfolglosigkeit hatte die Polizei die Überwachung nach einem Monat beendet.

Entgegen der Verpflichtung in der Strafprozessordnung (§ 101 Abs. 4 Nr. 12 StPO) war keine nachträgliche Information der beobachteten Bewohner erfolgt. Diese erfuhren zufällig durch einen in der Straße wohnenden Nachbarn, bei dem die Polizei die Videoanlage hatte installieren wollen, von der polizeilichen Absicht. Erst durch Einschaltung des Landesdatenschutzbeauftragten von Baden-Württemberg war bekannt worden, dass die Polizei ihre Absicht tatsächlich auch realisiert hatte.

Das LG Tübingen stellte fest, dass die Videoüberwachung wegen fehlender richterlicher Anordnung gem. § 163f Abs. 1 Nr. 1 StPO rechtswidrig war und bestätigte damit auch die Ansicht des Landesdatenschutzbeauftragten. Der Rechtsanwalt der Bewohner und Vorsitzende der Humanistischen Union Landesverband Baden-Württemberg, Dr. Udo Kauß, erklärte: „Die nach Bekanntwerden der Videoüberwachung beantragte richterliche Überprüfung zeigt, dass sich auch eine nachträgliche juristische Gegenwehr durchaus lohnen kann. Es gilt leider immer wieder aufs Neue, der Polizei klar zu machen, dass sie nicht in eigener Machtvollkommenheit über die Grundrechte von Bürgern befinden kann, auch wenn es sich um Angehörige der sog. linksautonomen Szene handelt" (PE Humanistische Union, LV Baden-Württemberg v. 16.06.2020, Polizeiliche Langzeit-Videoüberwachung von zwei Tübinger Wohnprojekten unzulässig).

**ArbG Bonn**

## Allgemeine Frage nach Vorstrafen bei Bewerbung unzulässig

Das Arbeitsgericht Bonn (ArbG) hat auf die Klage eines Auszubildenden hin mit Urteil vom 20.05.2020 entschieden, dass ein Arbeitgeber von einem Stellenbewerber keine allgemeine Auskunft über Vorstrafen und Ermittlungsverfahren verlangen darf (Az. 5 Ca 83/20). Der Arbeitgeber darf demgemäß dazu nur dann Informationen einholen, wenn diese für den zu besetzenden Arbeitsplatz relevant sein könnten. Der Kläger hatte eine Ausbildung als Fachkraft für Lagerlogistik begonnen. Bei dieser Tätigkeit hatte er auch Zugriff auf hochwertige Vermögensgüter der Beklagten. Im Rahmen des Einstellungsverfahrens hatte der Kläger auf einem sogenannten Personalblatt bei der Frage nach „Gerichtlichen Verurteilungen/schwebenden Verfahren" die Antwort „Nein" angekreuzt. Tatsächlich wusste er zu dem Zeitpunkt jedoch, dass ihm ein Strafprozess wegen Raubes bevorstand.

Etwa ein Jahr nach seiner Einstellung teilte der Kläger seinem Vorgesetzten mit, dass er eine Haftstrafe antreten müsse und eine Erklärung benötige, dass er seine Ausbildung während seines Freigangs fortführen könne. Daraufhin wollte der Arbeitgeber den Ausbildungsvertrag wegen arglistiger Täuschung anfechten. Dies wies das ArbG zurück. Die von der Beklagten unspezifisch gestellte Frage nach Ermittlungsverfahren jeder Art sei bei einer Bewerbung um eine Ausbildungsstelle als Fachkraft für Lagerlogistik zu weitgehend und damit unzulässig. Nicht jede denkbare Straftat begründe Zweifel an der Eignung des Klägers für diese Ausbildung. Die Entscheidung ist noch nicht rechtskräftig. (Arbeitgeber: Bewerber nicht allgemein nach Vorstrafen fragen, www.rtl.de 27.05.2020).

**LG Wien**

## Schadenersatz wegen Auskunftsverweigerung und nicht mehr

Max Schrems bekommt gemäß einem Urteil des Landesgerichts für Zivilrechtssachen Wien (LG) vom 30.06.2020 500 Euro Schadenersatz, weil Facebook sich geweigert hat, umfassend Auskunft zu erteilen. Außerdem muss Facebook binnen 14 Tagen die rechtlich erforderliche Auskunft erteilen (3 Cg 52/14k-91). Alle anderen Vorwürfe Schrems' weist das Gericht ab. Zuvor hatte sich die Richterin bereits zweimal für unzuständig erklärt, was vom EuGH bzw. Österreichs Oberstem Gerichtshofs (OGH) jedes Mal aufgehoben wurde.

Nun gibt es nach sechs Jahren Prozessdauer das erste Urteil. Das Gericht legt auf dutzenden Seiten den Sachverhalt dar, um dann mit einer sehr kurzen Begründung zu überraschen. Es spricht Schrems das Recht auf Vertragsabschluss und Weisungsgebung im Bereich der Verarbeitung jener Daten ab, die er selbst zu Facebook hochgeladen oder dort erzeugt hat. Auf Datenverarbeitung für private oder familiäre Tätigkeiten sei die DSGVO nicht anwendbar,

weshalb Schrems daraus keine Rechte ableiten könne.

Darüber hinausgehende Datenverarbeitung seitens Facebook habe Schrems entweder nicht beweisen können oder durch seinen Vertragsabschluss mit Facebook akzeptiert. Er könne den Vertrag durch Löschung seines Facebook-Kontos jederzeit beenden. Im Ergebnis sieht die Richterin „keine rechtswidrigen Datenverarbeitungsvorgänge“ bei Facebook.

Artikel 9 DSGVO verbietet unter anderem die Verarbeitung von Daten über sexuelle Orientierung und politische Meinung (mit Ausnahmen). Facebook hat Schrems unstrittig Werbung gezeigt, die in Bezug zu seiner sexuellen Orientierung steht, und Schrems Einladungen zu bestimmten politischen Veranstaltungen vermittelt. Aus Sicht der Richterin ist aber beides nicht zu beanstanden: Schrems habe seine sexuelle Orientierung selbst öffentlich gemacht. Und dass Facebook auswertet, für welche Politiker und Parteien sich Schrems interessiere, sei keine Verarbeitung von Daten über seine politische Meinung. Schrems könne ja auch Seiten von Parteien aufgerufen haben, deren Meinung er nicht teile.

Somit blieb nur, dass Facebook seiner Auskunftsverpflichtung trotz mehrmaliger Aufforderung jahrelang nicht ausreichend nachgekommen ist. Dafür muss Facebook nun Schrems, der unbezahlter Vorsitzender der Datenschutzorganisation noyb.eu ist, 500 Euro Schadenersatz zahlen und die Auskunft erteilen. Facebook musste eingestehen, dass es seinen Nutzern auch in den einschlägigen „Tools“ nicht alle Daten zeigt, die es über die Nutzer sammelt und verwertet. Es werden nur Daten gezeigt, von denen Facebook meint, dass sie für die Nutzer „relevant“ seien.

Die Richterin meint, dass die Mehrheit der User personalisierte Reklame lieber hat als nicht zugeschnittene Werbung. Im Verfahren hatte Cecilia Alvarez, bei Facebook für Datenschutz in Europa, dem Nahen Osten und Afrika zuständig, als Zeugin ausgesagt. Auch mit ihrer Hilfe konnte nicht geklärt werden, warum Facebook GPS-Daten Schrems‘ hatte. Wie Facebook konkret Daten technisch verarbeitet und löscht, konnte Alvarez ebenfalls nicht erklären. Eine weitere geladene Facebook-Managerin hatte sich geweigert, vor dem Wiener Gericht zu erscheinen. Laut Urteil ist ihre Zeugenaussage nicht erzwingbar.

Während Facebook das Urteil noch prüft, hat Schrems bereits entschieden, in Berufung zu gehen: „Die Richterin hat schon in der Verhandlung gesagt, dass sie sich auf die Fakten konzentriert, weil die kniffligen rechtlichen Fragen ohnehin von den höheren Gerichten geklärt werden. Die Entscheidung ist aber trotzdem etwas grotesk: Die illegalen Datenverarbeitungen von Facebook werden auf 36 Seiten beschrieben; aber nur in gerade 19 Sätzen werden fast alle Klagepunkte pauschal abgewiesen. Nur eine volle Auskunft zu meinen Daten und € 500 symbolischen Schadenersatz soll ich bekommen. Mit den kniffligen Fragen ob das Vorgehen von Facebook nach der DSGVO legal ist, wollte sich die Richterin wohl einfach nicht beschäftigen“ (Sokolov, Wiener Gericht findet bei Facebook „keine rechtswidrige Datenverarbeitung“, www.heise.de 02.07.2020, Kurzlink: https://heise.de/-4801389).

# Buchbesprechungen




Joachim Jahn, Micha Guttmann und Jürgen Krais
**Krisenkommunikation bei Compliance-Verstößen**
München 2020, C.H. Beck Verlag

(me) Wie wichtig das Thema Compliance geworden ist, zeigen die jüngsten Ermittlungen zur Aufklärung des Cum-Ex-Skandals und die Reaktionen der betroffenen Banken dazu.

Wenn Compliance im Mindeststandard die Einhaltung des mit staatlichen Sanktionen bewehrten Rechts bedeutet, gehört der Datenschutz dazu. Dass es hier zu rechtserheblichen Vorfällen kommen kann, ist nicht erst seit dem Screening der Beschäftigten der Deutschen Bahn in den Jahren 2002/2003 bekannt.

Das vorzustellende Werk ist ein Handbuch aus der Reihe „Compliance für die Praxis“. Diese Bezeichnung ist Programm; im vorliegenden Handbuch darf sie als geglückt bezeichnet werden. In geordneter und übersichtlicher Weise wird dargestellt, wie Kommunikation als intelligentes Werkzeug in Compliance-Vorfällen eingesetzt wird und welche Fehler zu vermeiden sind. Auch die Einordnung als Handbuch, also als thematische Zusammenstellung von Wissen zum Thema, ist zutreffend.

Der Beck Verlag ist zu Autoren- und Themenwahl zu beglückwünschen. Zwar gibt es zahlreiche Bücher zum Thema „Compliance“. Man denke nur an den im gleichen Verlag erschienenen Klassiker von Moosmayer, der im nächstes Jahr in der 4. Auflage erscheinen wird, sowie an zahllose andere. Und doch wird durch das Handbuch zum Thema „Kommunikation im Compliance-Fall“ eine Lücke geschlossen. Denn das Handbuch ist für den im Unternehmen Tätigen geschrieben: Nach einer Beschreibung der Compliance-Organisation und ihrer Einbettung in das Unternehmen wird die Krise (= Compliance-Vorfall) beschrieben, wie man sich darauf vorbereiten kann, welche Kommunikationspläne zu erstellen sind und wie mit Krisen im Einzelfall umgegangen werden kann, wobei die Differenzierung nach Zielgruppen überaus sinnvoll ist. Differenziert wird auch nach Art des Unternehmens bzw. der Organisation, die betroffen ist (börsennotiertes Unternehmen, Unternehmen der öffentlichen Hand, Verein,

u.a.). Erläutert wird, wie „die Medien", also insbesondere wie Journalisten arbeiten und nach welchen Gesetzmäßigkeiten eine sog. „Medienkampagne" ablaufen kann. All das ist sehr lehrreich und kurzweilig dargestellt und auch für den Laien äußerst interessant. Man merkt der Darstellung an, dass sie von erfahrenen Compliance-Fachleuten geschrieben wurde. Dr. Thomas Kremer, Vorstandsmitglied der Deutschen Telekom AG, zuständig für Datenschutz und Compliance, lobt in seinem Vorwort zu Recht, dass der Leser in dem Handbuch seine „eigene Kommunikationslösung" finden wird. Im Grunde geht es dabei um die Beantwortung der Frage, wie sich Unternehmen und die Unternehmensführung im Compliance-Fall verhalten sollen. Ziel ist dabei die Deutungshoheit über die Ereignisse zu behalten oder zurückzugewinnen.

Abgerundet wird die mit zahllosen Beispielen und Bezügen aus der jüngeren Vergangenheit versehene Darstellung mit einem „praktischen Fall", der die Erläuterungen der ersten 65 Seiten veranschaulicht. Zum Ende folgen Checklisten sowie Interviews mit dem Investigativ-Journalisten Klaus Ott, der früheren Justizministerin in NRW, Roswitha Müller-Piepenkötter, sowie dem ehem. Chief Compliance Officer der Deutschen Bahn AG und einer ehem. Staatsanwältin, die heute als Fachanwältin für Strafrecht arbeitet. Die Verwendung von Interviews mag ungewöhnlich erscheinen, ist aber gelungen, da sie in leicht lesbarer Weise die unterschiedlichen Perspektiven der im Bereich der Compliance Tätigen (investigativ arbeitenden Journalisten, für einen Compliance-Fall verantwortliche Ministerin, im Bereich tätige Anwälte bzw. Compliance Officer) aufzeigt.

Abschließend ist der Pressecodex des Deutschen Presserates abgedruckt.

Das Handbuch zur Krisenkommunikation bei Compliance-Verstößen ist ein exzellenter Ratgeber für die Praxis, dem ein Platz in jedem Bücherregal von Unternehmen und Organisationen zu wünschen ist!




**Grundfragen des Verwaltungsverfahrensrechts im deutsch-taiwanesischen Rechtsvergleich**
hg. von Matthias Knauff und Chien-Hung Liu, Schriftenreihe des Hellmuth-Loening-Zentrums für Staatswissenschaften Jena, Band 25, Berlin 2020

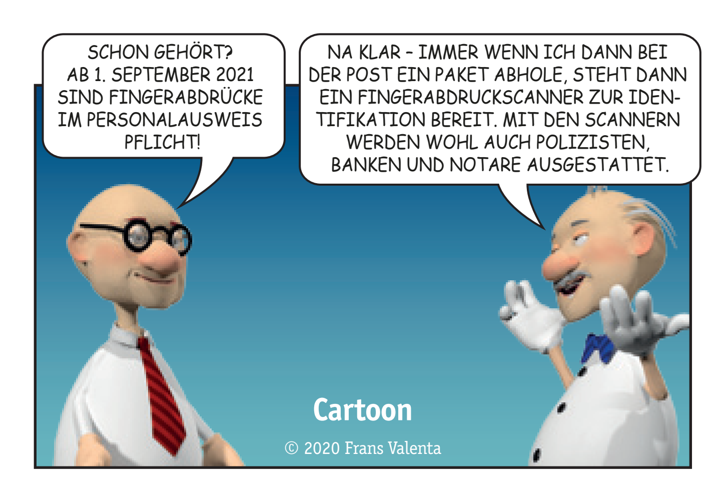
(me) Beim Datenschutzrecht handelt es sich um (besonderes) Verwaltungsrecht. Insoweit war es nicht abwegig, in der DANA einen Tagungsband zur rechtsvergleichenden Betrachtung des deutschen und des taiwanesischen Verwaltungsverfahrensrechts vorzustellen.

Die Tagung fand im Sommer 2018 in Jena statt. Die dazu gehörende Publikation enthält Vorträge deutscher und taiwanesischer Rechtswissenschaftler.

Besonders interessant für DANA-Leser dürfte der Beitrag des Dekans der Chung-Cheng-Nationaluniversität sein: Professor Chien-Hung Liu referiert über die aus deutscher Sicht recht progressive (digitale) Bürgerbeteiligung im taiwanesischen Verwaltungsverfahren. Zwar ist auch manchem Zeitungsleser in Europa nicht verborgen geblieben, dass die Entwicklungen der sogenannten Digitalisierung in der taiwanesischen Gesellschaft sehr weit fortgeschritten sind. Dafür sorgen schon die Darstellungen Audrey Tangs, der Digitalisierungsministerin des Landes, die regelmäßig in der überregionalen Presse Europas auftaucht. Dennoch ist erstaunlich, wie weit verschiedene Formen der digitalen Bürgerbeteiligung gediehen sind, was wohl insbesondere auf die Sonnenblumen-Proteste, einer studentischen Protestbewegung von 2014, zurückgehen dürfte. Da gibt es Online-Petitionen (join.gov.tw), die Online-Konferenz zur Verbesserung der Transparenz von Regierungshandlungen (vTaiwan) und nicht das zuletzt die regionale Mitbestimmung der Hauptstadtbewohner über die Verteilung und Zuweisung staatlicher finanzieller Mittel (participatory budgeting). Welche Dynamik sich hier entfaltet, wird man in näherer Zukunft beobachten können.

Auch die anderen Vorträge zu Themen wie Verwaltungsvertrag und Planfeststellung lesen sich interessant und stellen ihr jeweiliges Thema zum Teil kontrovers dar.

Wünschenswert wäre eine Tagung dieser Art und Güte zum Datenschutz.








**Verpflichtende Fingerabdrücke in Personalausweisen gab es zuletzt zur Zeit des Nationalsozialismus ab 1938**

**Wer sich gegen die Neuauflage mit einer Petition wehren möchte:**

**https://aktion.digitalcourage.de/perso-ohne-finger**